Contact Information
Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation
• For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal www.paloaltonetworks.com/documentation.
• To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
• Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright
Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2017- Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised
# Table of Contents

**Traps Overview**
- About Traps ....................................................................................................................... 11
- Malware Protection Overview ............................................................................................ 11
- Exploit Protection Overview .............................................................................................. 12

**Traps Components**
- ESM Console .......................................................................................................................... 13
- ESM Server .............................................................................................................................. 13
- Database .................................................................................................................................. 14
- Endpoints .................................................................................................................................. 14
- Traps Agent ............................................................................................................................... 14
- External Logging Platform ..................................................................................................... 15
- WildFire ..................................................................................................................................... 15
- Forensic Folder ......................................................................................................................... 16

**Traps Deployment Scenarios**
- Standalone Deployment ........................................................................................................ 19
- Small Deployments ................................................................................................................ 20
  - Small Single-Site Deployment ............................................................................................ 20
  - Small Multi-Site Deployment ............................................................................................. 21
- Large Deployments ................................................................................................................ 22
  - Large Single-Site Deployment .......................................................................................... 22
  - Large Multi-Site Deployment with One Endpoint Security Manager .................................. 23
  - Large Multi-Site Deployment with Roaming Agents (Without VPN) .................................. 24
  - Large Multi-Site Deployment with Roaming Agents (With VPN) ....................................... 25

**Prerequisites**
- Hardware Requirements ......................................................................................................... 29
  - Standalone Endpoint Security Manager Hardware Requirements ........................................ 29
  - Distributed Endpoint Security Manager Hardware Requirements ....................................... 29
- Traps Hardware Requirements ................................................................................................ 31
- Software Requirements .......................................................................................................... 32
  - ESM Console Software Requirements .............................................................................. 32
  - ESM Server Software Requirements .................................................................................. 32
  - Database Software Requirements ........................................................................................ 33
  - Traps Software Requirements ............................................................................................. 33

**Set Up the Traps Infrastructure**
- Set Up the Endpoint Infrastructure ..................................................................................... 37
  - Endpoint Infrastructure Installation Considerations .......................................................... 38
  - TLS/SSL Encryption for Traps Components ......................................................................... 38
  - Configure the MS-SQL Server Database .......................................................................... 39
  - Install the Endpoint Security Manager Server Software ............................................... 41
  - Install the Endpoint Security Manager Console Software ............................................. 44
  - Set Up the Endpoints ............................................................................................................ 47
    - Recommended Traps Deployment Process ....................................................................... 47
    - Traps Installation Options ............................................................................................... 48
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Traps on Windows Endpoints</td>
<td>48</td>
</tr>
<tr>
<td>Install Traps Components Using Msiexec</td>
<td>50</td>
</tr>
<tr>
<td>Install Traps Components</td>
<td>50</td>
</tr>
<tr>
<td>Uninstall Traps Components</td>
<td>51</td>
</tr>
<tr>
<td>Verify a Successful Installation</td>
<td>52</td>
</tr>
<tr>
<td>Verify Connectivity from the Endpoint</td>
<td>52</td>
</tr>
<tr>
<td>Verify Connectivity from the ESM Console</td>
<td>52</td>
</tr>
<tr>
<td>Manage Traps in a VDI Environment</td>
<td>53</td>
</tr>
<tr>
<td>VDI Overview</td>
<td>55</td>
</tr>
<tr>
<td>Virtualized Applications and Desktops</td>
<td>55</td>
</tr>
<tr>
<td>VDI Modes</td>
<td>55</td>
</tr>
<tr>
<td>VDI Installation Considerations</td>
<td>57</td>
</tr>
<tr>
<td>VDI Agent Licenses</td>
<td>57</td>
</tr>
<tr>
<td>Best Practices for VDI Deployments</td>
<td>58</td>
</tr>
<tr>
<td>Set Up Traps in a VDI Environment</td>
<td>59</td>
</tr>
<tr>
<td>Configure the Master Policy</td>
<td>61</td>
</tr>
<tr>
<td>Prerequisites for Configuring the Master Policy</td>
<td>61</td>
</tr>
<tr>
<td>Use the Traps VDI Tool to Configure the Master Policy</td>
<td>62</td>
</tr>
<tr>
<td>Traps VDI Tool CLI</td>
<td>64</td>
</tr>
<tr>
<td>Configure Traps Settings</td>
<td>66</td>
</tr>
<tr>
<td>Configure Traps for a Non-Persistent Storage Scenario</td>
<td>66</td>
</tr>
<tr>
<td>Configure Traps for a Persistent Storage Scenario</td>
<td>67</td>
</tr>
<tr>
<td>Tune and Test the VDI Policy</td>
<td>69</td>
</tr>
<tr>
<td>Administer the ESM Server</td>
<td>71</td>
</tr>
<tr>
<td>Manage ESM Server Settings</td>
<td>73</td>
</tr>
<tr>
<td>Manage ESM Console Settings</td>
<td>75</td>
</tr>
<tr>
<td>Manage Multiple ESM Servers</td>
<td>76</td>
</tr>
<tr>
<td>Known Limitations with Multi-ESM Deployments</td>
<td>76</td>
</tr>
<tr>
<td>What Logic Does the Agent Use When Selecting an ESM Server?</td>
<td>76</td>
</tr>
<tr>
<td>Activate, Disable, or Delete an ESM Server</td>
<td>77</td>
</tr>
<tr>
<td>Traps Licenses</td>
<td>79</td>
</tr>
<tr>
<td>About Traps Licenses</td>
<td>79</td>
</tr>
<tr>
<td>Add a Traps License Using the ESM Console</td>
<td>79</td>
</tr>
<tr>
<td>Add a Traps License Using the DB Configuration Tool</td>
<td>80</td>
</tr>
<tr>
<td>Detach a Traps License</td>
<td>81</td>
</tr>
<tr>
<td>Manage Administrator Access to the ESM Console</td>
<td>82</td>
</tr>
<tr>
<td>Administrative Roles</td>
<td>82</td>
</tr>
<tr>
<td>Administrative Users</td>
<td>83</td>
</tr>
<tr>
<td>Administrative Authentication</td>
<td>84</td>
</tr>
<tr>
<td>Configure Administrative Accounts and Authentication</td>
<td>84</td>
</tr>
<tr>
<td>Export and Import Policy Files</td>
<td>88</td>
</tr>
<tr>
<td>User-Defined Rules</td>
<td>88</td>
</tr>
<tr>
<td>Content Updates</td>
<td>89</td>
</tr>
<tr>
<td>Monitoring</td>
<td>91</td>
</tr>
<tr>
<td>Maintain the Endpoints and Traps</td>
<td>93</td>
</tr>
<tr>
<td>Use the Endpoint Security Manager Dashboard</td>
<td>94</td>
</tr>
<tr>
<td>Monitor Security Events</td>
<td>95</td>
</tr>
<tr>
<td>Use the Security Events Dashboard</td>
<td>95</td>
</tr>
<tr>
<td>View the Security Event History on an Endpoint</td>
<td>98</td>
</tr>
</tbody>
</table>
## Malware Protection

- Malware Protection Concepts... 123
- ESM Forwarding... 123
- Verdicts... 123
- Verdict Caches... 123
- File Type Analysis... 124

## Malware Protection Policy Best Practices

- Phase 1: Evaluation of Hash Verdicts... 126
- Phase 2: Evaluation of the Restriction Policy... 128
- Phase 3: Evaluation of the Malware Protection Policy... 128

## WildFire Integration

- Set Up the ESM to Communicate with WildFire... 129
- Configure a WildFire Rule... 130

## Manage Hashes for Executable Files

- View and Search Hashes... 133
- Export and Import Hashes... 133
- View a WildFire Report... 134
- Override a WildFire Verdict... 135
- Recheck a WildFire Decision... 135
- Report an Incorrect Verdict... 136
- Upload a File to WildFire for Analysis... 136
- Manage Quarantine Settings... 137
- Restore a Quarantined File... 137
- Manage Restrictions on Executable Files... 139

## Monitor the Endpoints

- View Endpoint Health Details... 100
- View Notifications About Changes in the Agent Status... 100
- View the Status of the Agent from the Traps Console... 101
- View the Rule History of an Endpoint... 102
- View Changes to the Security Policy from the Traps Console... 102
- View the Service Status History of an Endpoint... 103
- Remove an Endpoint from the Health Page... 103

## Monitor the ESM Servers

- View the Health of the ESM Servers... 104
- View Notifications About the ESM Server... 104
- View the Rule Summary... 106
- Monitor Forensics Retrieval... 107

## Getting Started with Rules

- Endpoint Policy Rule Concepts... 111
- Policy Rule Types... 112
- Policy Enforcement... 112
- Common Rule Components and Actions... 114
  - Conditions... 114
  - Target Objects... 116
  - Name or Rename a Rule... 117
  - Save Rules... 117
  - Manage Saved Rules... 118
  - Filter Rules... 119
  - Disable or Enable All Protection Rules... 120
  - Show or Hide the Default Policy Rules... 120

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor the Endpoints...</td>
<td>100</td>
</tr>
<tr>
<td>View Endpoint Health Details...</td>
<td>100</td>
</tr>
<tr>
<td>View Notifications About Changes in the Agent Status...</td>
<td>100</td>
</tr>
<tr>
<td>View the Status of the Agent from the Traps Console...</td>
<td>101</td>
</tr>
<tr>
<td>View the Rule History of an Endpoint...</td>
<td>102</td>
</tr>
<tr>
<td>View Changes to the Security Policy from the Traps Console...</td>
<td>102</td>
</tr>
<tr>
<td>View the Service Status History of an Endpoint...</td>
<td>103</td>
</tr>
<tr>
<td>Remove an Endpoint from the Health Page...</td>
<td>103</td>
</tr>
<tr>
<td>Monitor the ESM Servers...</td>
<td>104</td>
</tr>
<tr>
<td>View the Health of the ESM Servers...</td>
<td>104</td>
</tr>
<tr>
<td>View Notifications About the ESM Server...</td>
<td>104</td>
</tr>
<tr>
<td>View the Rule Summary...</td>
<td>106</td>
</tr>
<tr>
<td>Monitor Forensics Retrieval...</td>
<td>107</td>
</tr>
<tr>
<td>Getting Started with Rules...</td>
<td>109</td>
</tr>
<tr>
<td>Endpoint Policy Rule Concepts...</td>
<td>111</td>
</tr>
<tr>
<td>Policy Rule Types...</td>
<td>112</td>
</tr>
<tr>
<td>Policy Enforcement...</td>
<td>112</td>
</tr>
<tr>
<td>Common Rule Components and Actions...</td>
<td>114</td>
</tr>
<tr>
<td>Conditions...</td>
<td>114</td>
</tr>
<tr>
<td>Target Objects...</td>
<td>116</td>
</tr>
<tr>
<td>Name or Rename a Rule...</td>
<td>117</td>
</tr>
<tr>
<td>Save Rules...</td>
<td>117</td>
</tr>
<tr>
<td>Manage Saved Rules...</td>
<td>118</td>
</tr>
<tr>
<td>Filter Rules...</td>
<td>119</td>
</tr>
<tr>
<td>Disable or Enable All Protection Rules...</td>
<td>120</td>
</tr>
<tr>
<td>Show or Hide the Default Policy Rules...</td>
<td>120</td>
</tr>
<tr>
<td>Malware Protection...</td>
<td>121</td>
</tr>
<tr>
<td>Malware Protection Concepts...</td>
<td>123</td>
</tr>
<tr>
<td>ESM Forwarding...</td>
<td>123</td>
</tr>
<tr>
<td>Verdicts...</td>
<td>123</td>
</tr>
<tr>
<td>Verdict Caches...</td>
<td>123</td>
</tr>
<tr>
<td>File Type Analysis...</td>
<td>124</td>
</tr>
<tr>
<td>Malware Protection Policy Best Practices...</td>
<td>125</td>
</tr>
<tr>
<td>Malware Protection Flow...</td>
<td>126</td>
</tr>
<tr>
<td>Phase 1: Evaluation of Hash Verdicts...</td>
<td>126</td>
</tr>
<tr>
<td>Phase 2: Evaluation of the Restriction Policy...</td>
<td>128</td>
</tr>
<tr>
<td>Phase 3: Evaluation of the Malware Protection Policy...</td>
<td>128</td>
</tr>
<tr>
<td>WildFire Integration...</td>
<td>129</td>
</tr>
<tr>
<td>Set Up the ESM to Communicate with WildFire...</td>
<td>129</td>
</tr>
<tr>
<td>Configure a WildFire Rule...</td>
<td>130</td>
</tr>
<tr>
<td>Manage Hashes for Executable Files...</td>
<td>133</td>
</tr>
<tr>
<td>View and Search Hashes...</td>
<td>133</td>
</tr>
<tr>
<td>Export and Import Hashes...</td>
<td>133</td>
</tr>
<tr>
<td>View a WildFire Report...</td>
<td>134</td>
</tr>
<tr>
<td>Override a WildFire Verdict...</td>
<td>135</td>
</tr>
<tr>
<td>Recheck a WildFire Decision...</td>
<td>135</td>
</tr>
<tr>
<td>Report an Incorrect Verdict...</td>
<td>136</td>
</tr>
<tr>
<td>Upload a File to WildFire for Analysis...</td>
<td>136</td>
</tr>
<tr>
<td>Manage Quarantine Settings...</td>
<td>137</td>
</tr>
<tr>
<td>Restore a Quarantined File...</td>
<td>137</td>
</tr>
<tr>
<td>Manage Restrictions on Executable Files...</td>
<td>139</td>
</tr>
</tbody>
</table>
Restriction Rules........................................................................................................... 139
Wildcards and Variables in Restriction Rules......................................................... 140
Add a New Restriction Rule..................................................................................... 144
Manage Global Whitelists........................................................................................ 145
Block Execution from Local Folders........................................................................ 147
Block Execution from Network Folders................................................................. 148
Define External Media Restrictions and Exemptions.............................................. 149
Define Child Process Restrictions.......................................................................... 150
Define Java Restrictions and Exemptions.............................................................. 151
Define Unsigned Executable File Restrictions and Exemptions............................ 152
Manage Malware Protection Rules.......................................................................... 154
Malware Protection Rules....................................................................................... 154
Configure Thread Injection Protection................................................................. 155
Manage the Thread Injection Whitelist.................................................................... 157
Configure Suspend Guard Protection........................................................................ 157
Manage the Suspend Guard Whitelist...................................................................... 159

Exploit Protection.................................................................................................... 161
Manage Processes.................................................................................................... 163
Process Protection Types........................................................................................ 163
Processes Protected by the Default Policy.............................................................. 163
Add a New Protected Process.................................................................................. 164
Import or Export a Process...................................................................................... 165
View, Modify, or Delete a Process............................................................................ 166
View Processes Currently Protected by Traps.......................................................... 166
Manage Exploit Protection Rules............................................................................. 168
Exploit Protection Rules........................................................................................ 168
Exploit Protection Rule Hierarchy............................................................................ 168
Exploit Protection Modules (EPMs)......................................................................... 168
Default Exploit Protection Policy............................................................................ 170
Create an Exploit Protection Rule........................................................................... 171
Exclude an Endpoint from an Exploit Protection Rule.............................................. 173

Manage the Endpoints.............................................................................................. 175
Manage Traps Action Rules....................................................................................... 177
Traps Action Rules.................................................................................................. 177
Add a New Action Rule........................................................................................... 177
Manage Data Collected by Traps............................................................................. 178
Uninstall or Upgrade Traps on the Endpoint........................................................... 180
Update or Revoke the Traps License on the Endpoint............................................. 181
Manage Agent Settings Rules.................................................................................. 182
Traps Agent Settings Rules..................................................................................... 182
Add a New Agent Settings Rule............................................................................... 183
Define Event Logging Preferences........................................................................ 184
Hide or Restrict Access to the Traps Console.......................................................... 185
Define Communication Settings Between the Endpoint and the ESM Server........... 186
Collect New Process Information.......................................................................... 189
Manage Service Protection...................................................................................... 190
Change the Uninstall Password.............................................................................. 191
Create a Custom User Alert Message...................................................................... 192

Forensics.................................................................................................................... 195
Troubleshooting.............................................................................................. 287
  Traps Troubleshooting Resources............................................................... 289
  Traps and Endpoint Security Manager Processes..................................... 291
  ESM Tech Support File.................................................................................. 292
  Database (DB) Configuration Tool.............................................................. 293

Reports and Logging...................................................................................... 211
  Event Log Types.......................................................................................... 213
    Security Events.......................................................................................... 213
    Policies - General...................................................................................... 214
    Policies - Rules.......................................................................................... 215
    Policies - Process Management................................................................. 215
    Policies - Restriction Settings................................................................. 216
    Policies - Hash Control............................................................................. 216
    Monitor - Agent......................................................................................... 217
    Monitor ESM............................................................................................ 221
    Settings - Administration......................................................................... 222
    Settings - Agent......................................................................................... 223
    Settings - ESM.......................................................................................... 224
    Settings - Conditions................................................................................ 224
    Settings - Licenses.................................................................................... 224
  Common Variables Used in Events.............................................................. 227
    Agent Change Event Variables................................................................. 227
    ESM Configuration Change Event Variables.......................................... 227
    Policy Change Event Variables................................................................. 228
    ESM Server Event Variables..................................................................... 229
    Security Event Monitoring Variables...................................................... 229
  Forward Logs to an External Logging Platform.......................................... 231
    Enable Log Forwarding to an External Logging Platform...................... 231
    Enable Log Forwarding to an External Logging Platform Using the DB Configuration Tool........................................................................ 232
    CEF Format............................................................................................... 233
    LEEF Format............................................................................................. 246
    Syslog (RFC5424) Format.......................................................................... 259
  Forward Logs to Email.................................................................................. 270
    Enable Log Forwarding to Email.............................................................. 270
    Email Format............................................................................................. 271

Forensics Overview....................................................................................... 197
  Forensics Flow........................................................................................... 197
  Forensic Data Types................................................................................... 198
  Best Practices for Managing Forensic Data.............................................. 200
  Manage Forensics Rules and Settings..................................................... 201
    Forensics Rules......................................................................................... 201
    Change the Default Forensic Folder......................................................... 201
    Create a Forensics Rule........................................................................... 203
    Define Memory Dump Preferences......................................................... 204
    Define Forensics Collection Preferences............................................... 205
    Retrieve Data About a Security Event..................................................... 206
  Agent Query................................................................................................. 208
    Agent Query Flow..................................................................................... 208
    Search Endpoints for a File, Folder, or Registry Key.............................. 208
    View the Results of an Agent Query....................................................... 209

Forensics Flow............................................................................................... 197

Forensic Data Types..................................................................................... 198

Best Practices for Managing Forensic Data.............................................. 200

Manage Forensics Rules and Settings..................................................... 201

Forensics Rules......................................................................................... 201

Change the Default Forensic Folder......................................................... 201

Create a Forensics Rule........................................................................... 203

Define Memory Dump Preferences......................................................... 204

Define Forensics Collection Preferences............................................. 205

Retrieve Data About a Security Event.................................................... 206

Agent Query................................................................................................. 208

Agent Query Flow..................................................................................... 208

Search Endpoints for a File, Folder, or Registry Key.............................. 208

View the Results of an Agent Query....................................................... 209

Access the Database Configuration Tool............................................................................ 293
Configure Administrative Access to the ESM Console Using the DB Configuration Tool................................................................................................................................................294
Configure ESM Server Settings Using the DB Configuration Tool................................295
Customizable ESM Server Settings....................................................................................... 296
Cytool.........................................................................................................................................................299
Access Cytool............................................................................................................................. 299
View Processes Currently Protected by Traps Using Cytool..........................................300
Manage Protection Settings on the Endpoint Using Cytool............................................. 300
Manage Traps Drivers and Services on the Endpoint Using Cytool....................................303
View and Compare Security Policies on an Endpoint Using Cytool................................306
Manage Logging of Traps Components Using Cytool...................................................... 307
Restore a Quarantined File Using Cytool............................................................................308
View Statistics for a Protected Process Using Cytool..................................................... 309
View Details About the Traps Local Analysis Module Using Cytool............................. 310
View Hash Details About a File Using Cytool....................................................................310
Troubleshoot Traps Issues................................................................................................................... 312
  Why can't I install Traps?........................................................................................................ 312
  Why can't I upgrade or uninstall Traps?........................................................................... 312
  Why can't Traps connect to the ESM Server?.................................................................... 313
  How do I fix a Traps server certificate error?..................................................................... 315
Troubleshoot ESM Console Issues............................................................................................. 316
  Why can't I log in to the ESM Console?.............................................................................. 316
  Why do I get a server error when launching the ESM Console?................................... 317
  Why do all endpoints appear as disconnected in the ESM Console?..............................317
Traps Overview

Traps™ replaces antiquated antivirus solutions by preventing advanced persistent threats (APTs) and zero-day attacks. Traps also provides protection for your endpoints by blocking attack vectors before any malware is initiated or software vulnerabilities or bugs are exploited.

The following topics describe the Traps solution in more detail:

> About Traps
> Traps Components
About Traps

Cyberattacks are attacks performed on networks or endpoints to inflict damage, steal information, or achieve other goals that involve taking control over computer systems that do not belong to the attackers. Adversaries perpetrate cyberattacks either by causing a user to unintentionally run a malicious executable file or by exploiting a weakness in a legitimate executable file to run malicious code behind the scenes without the knowledge of the user.

One way to prevent these attacks is to identify executable files, dynamic-link libraries (DLLs), or other pieces of code as malicious and then prevent them from executing by testing each potentially dangerous code module against a list of specific, known threat signatures. The weakness of this method is that it is time-consuming for signature-based antivirus (AV) solutions to identify newly created threats that are known only to the attacker (also known as zero-day attacks or exploits) and add them to the lists of known threats, which leaves endpoints vulnerable until signatures are updated.

The Traps solution takes a more effective and efficient approach to preventing attacks thus eliminating the need for traditional AV. Rather than try to keep up with the ever-growing list of known threats, Traps sets up a series of roadblocks that prevent the attacks at their initial entry points—that point where legitimate executable files are about to unknowingly allow malicious access to the system.

Traps targets software vulnerabilities in processes that open non-executable files using exploit prevention techniques. Traps also uses malware prevention techniques to prevent malicious executable files from running. Using this two-fold approach, the Traps solution can prevent all types of attacks, whether they are known or unknown threats.

All aspects of endpoint security settings—the endpoints and groups to which settings are applied, the applications they protect, the defined rules, the restrictions, and the actions—are all highly configurable. This allows each organization to tailor Traps to its needs so that Traps can provide maximum protection with minimal disruption of day-to-day activities.

- Malware Protection Overview
- Exploit Protection Overview

Malware Protection Overview

Malicious executable files, known as malware, are often disguised as or embedded in non-malicious files. These files can attempt to gain control, gather sensitive information, or disrupt the normal operations of the system.

Traps prevents malware by reducing the attack surface and increasing the accuracy of malware detection. This approach combines several layers of protection, collectively known as the Malware Prevention Engine, that prevent known and unknown malware—including malicious Microsoft Windows screensaver files (.scr)—from infecting your endpoints. The Malware Prevention Engine automatically protects endpoints from malware whether your endpoints are online or offline, on-premise or off, connected to your organization’s network or not. The Malware Prevention Engine uses the following layers of protection:

- **WildFire integration**—Enables automatic detection of unknown malware and quickly prevents threats before an enterprise is compromised.
- **Evaluation of trusted signers**—Permits unknown executable files that are signed by trusted signers to run on the endpoint.
- **Local static analysis**—Enables Traps to use machine learning to analyze unknown executable files and issue a verdict. Traps uses the verdict returned by the local analysis module until it receives a verdict from the ESM Server.
- **Policy-based restrictions**—Enable you to block files from executing from specific local folders, network folders, or external media locations; limit or block child processes; block or whitelist Java processes initiated in web browsers; and block the execution of unsigned processes.
- **Malware protection modules**—Target specific malware behaviors and enable you to block the creation of remote threads.

For additional information, see **Malware Protection Flow**.

### Exploit Protection Overview

An exploit is a sequence of commands that take advantage of a bug or vulnerability in a software application or process. Attackers use these exploits as a means to access and use a system to their advantage. To gain control of a system, the attacker must take advantage of a chain of vulnerabilities in the system. Blocking any attempt to exploit a vulnerability in the chain will block the exploitation attempt entirely.

In a typical attack scenario, an attacker attempts to gain control of a system by first corrupting or bypassing memory allocation or handlers. Using memory-corruption techniques, such as buffer overflows and heap corruption, a hacker can trigger a bug in software or exploit a vulnerability in a process. The attacker must then manipulate a program to run code provided or specified by the attacker while evading detection. If the attacker gains access to the operating system, the attacker can then upload malware, such as Trojan horses (programs that contain malicious executable files), or otherwise use the system to their advantage. Traps prevents such exploit attempts by employing roadblocks or traps at each stage of an exploitation attempt.

When a user opens a non-executable file, such as a PDF or Word document, and the process that opened the file is protected, the Traps agent seamlessly injects code into the software. This occurs at the earliest possible stage before any files belonging to the process are loaded into memory. The Traps agent then activates one or more **Exploit Protection Modules (EPMs)** inside the protected process. The EPM targets a specific exploitation technique and is designed to prevent attacks on program vulnerabilities based on memory corruption or logic flaws.

Examples of attacks that the EPMs can prevent include dynamic-link library (DLL) hijacking (replacing a legitimate DLL with a malicious one of the same name), hijacking program control flow, and inserting malicious code as an exception handler.

In addition to automatically protecting processes from such attacks, Traps reports any prevention events to the Endpoint Security Manager, and performs additional actions according to the settings of the security policy rules. Common actions that Traps performs include collecting forensic data and notifying the user about the event. Traps does not perform any additional scanning or monitoring actions.

The default endpoint security policy protects the most vulnerable and most commonly used applications, but you can also add other third-party and proprietary applications to the list of protected processes. For more information, see **Add a New Protected Process**.

For more information, see **Manage Exploit Protection Rules**.
Traps Components

The Traps solution centers around the Endpoint Security Manager (ESM), which comprises an ESM Console, a database, an ESM Server, and the Traps agent protection software. The Traps agent is installed on each endpoint in your organization and, together, these components manage security policy rules, distribute the security policy to endpoints, and enforce the policy on the endpoints. The following diagram displays the Traps components and their relationships to each other and to other security components.

The following topics describe the Traps and other components in more detail.

- ESM Console
- ESM Server
- Database
- Endpoints
- Traps Agent
- External Logging Platform
- WildFire
- Forensic Folder

ESM Console

The Endpoint Security Manager (ESM) Console is a web interface that enables you to manage security events, monitor endpoint health, and configure policy rules from a web browser. The ESM Console communicates with the database independently from the ESM Server. You can install the ESM Console on the same server as the ESM Server, on a separate server, or on a cloud-based server.

As a best practice, use a single ESM Console to manage the ESM Server(s) in your Traps deployment. Using multiple ESM Consoles is not supported.

For information on hardware and software requirements for the ESM Console, see ESM Console Software Requirements.

ESM Server

The Endpoint Security Manager (ESM) Server functions as the connection server that relays information between the ESM components, including the Traps agent, and WildFire. Each ESM Server supports up to
16,000 Traps agents. In a multi-ESM deployment you can also install up to 5 ESM Servers to support up to 80,000 agents.

On a regular basis, the ESM Server retrieves the security policy from the database and distributes it to all Traps agents. Traps agents also relay security event information back to the ESM Server. For information on requirements for the ESM Server, see ESM Server Software Requirements.

Database

The database stores administrative information, security policy rules, endpoint history, and other information about security events. The database is managed over the MS-SQL platform. Each database requires a license and can communicate with one or more ESM Servers. The database may be installed on the same server as the ESM Console and ESM Server, such as in a standalone environment, or the database can be installed on a dedicated server. For information on hardware and software requirements for the database, see Database Software Requirements.

During evaluation we recommend you use SQL Server Express which enables you to easily migrate the database to SQL Server Standard or SQL Server Enterprise.

Endpoints

An endpoint is a Windows-based computer, server, virtual machine, tablet, or mobile device running the client-side protection application named Traps. For prerequisites, see Traps Software Requirements.

Traps Agent

The Traps agent protects the endpoint by enforcing your organization's security policy as defined in the Endpoint Security Manager. Depending on the configuration, Traps can protect against attempts to exploit software vulnerabilities and bugs and can prevent malicious executable files from running on your endpoints.

When a security event occurs on an endpoint, Traps collects forensic information about that event and, optionally, can also notify the user about the event and even display a custom notification message. On a regular basis, Traps communicates the status of the endpoint and transmits data related to any security events to the Endpoint Security Manager. The following table describes the types of messages that the Traps agent sends to the ESM Server:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps status</td>
<td>The Traps agent periodically sends messages to the ESM Server to indicate that it is operational and to request the latest security policy. The Notifications and Health pages in the Endpoint Security Manager display the status for each endpoint. The duration between messages, known as the heartbeat period, is configurable.</td>
</tr>
<tr>
<td>Notifications</td>
<td>The Traps agent sends notification messages about changes in the agent, such as when a service starts or stops, to the ESM Server. The server logs these notifications in the database and you can view the notifications in the ESM Console.</td>
</tr>
<tr>
<td>Updates</td>
<td>An end user can request an immediate policy update by clicking Check-in now on the Traps Console. This causes the Traps agent to request the latest security policy from the ESM Server without waiting for the end of the heartbeat period.</td>
</tr>
<tr>
<td>Message Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Prevention reports</td>
<td>If a prevention event occurs on an endpoint where the Traps agent is installed, the Traps agent reports all of event-related information to the ESM Server in real-time.</td>
</tr>
</tbody>
</table>

Traps also provides a user interface that you can use to view the protection status on the endpoint, security event history, running processes, and current security policy rules. Usually, a user will not need to run the Traps Console but the information can be useful when investigating a security-related event. If needed, you can choose to hide the console icon that launches the console or prevent users from launching the console from an endpoint altogether. If you provide access to the Traps Console, you can access it from the notification area (system tray) on an endpoint.

**External Logging Platform**

By using an external logging platform—such as security information and event management (SIEM) system or a syslog device—you can view aggregated logs from the ESM Console and ESM Servers. When enabled, the ESM component forwards reports about events to the external logging platform in addition to storing logs internally. The ESM component which forwards the logs varies depending on the type of event. For example, if you monitor verdict changes, the ESM Console sends logs when you override the verdict for a hash. If WildFire changes the verdict, the ESM Server sends the logs.

You can also integrate your external logging platform with third-party monitoring tools, such as Splunk, to analyze log data. Download the Splunk app for Palo Alto Networks at https://apps.splunk.com/app/491.

To add an external logging platform, see Forward Logs to an External Logging Platform.

**WildFire**

The Traps agent is designed to block attacks before any malicious code can run on the endpoint. While this approach ensures the safety of data and infrastructure, it enables the collection of forensic evidence only at the moment of prevention so cannot fully reveal the purpose of the attack or its entire flow.

The WildFire service is an optional, cloud-based malware analysis environment that turns unknown threats into known, preventable incidents. Enabling WildFire integration allows the Endpoint Security Manager to send any unknown executable files to WildFire and WildFire can then analyze the file, if needed, and respond with a verdict. If WildFire determined the executable file to be malicious, the Traps agent blocks the file from executing and notifies the Endpoint Security Manager about the event.

As WildFire detects new malware, it generates new signatures within the hour. Palo Alto Networks next-generation firewalls equipped with a WildFire subscription can receive the new signatures within minutes while firewalls with only a Threat Prevention subscription can still receive the new signatures in the next Antivirus signature update (within 24-48 hours).
If WildFire integration is enabled in the ESM Console, the Status page of the Traps Console displays a ✔️ next to Forensic Data Collection. If WildFire is not enabled, the Traps Console displays an ❌ next to Forensic Data Collection.

For more information, see Set Up the ESM to Communicate with WildFire and Malware Protection Flow.

Forensic Folder

When Traps encounters a security-related event, such as a file execution or an exploit attack, it logs real-time forensic details about the event on the endpoint. The forensic data includes the memory dump and other information associated with the event. You can retrieve the forensic data by creating an action rule to collect the data from the endpoint. After the endpoint receives the security policy that includes the action rule, the Traps agent sends all the forensic information to the forensic folder, which is sometimes referred to as the quarantine folder.

During the initial installation, you specify the path of the forensic folder that the Endpoint Security Manager uses to store forensic information it retrieves from endpoints. The Endpoint Security Manager supports multiple forensic folders and enables the Background Intelligent Transfer Service (BITS) on the folder during installation. If the forensic folder specified during installation cannot be reached, Traps defaults to the forensic folder specified in the ESM Console. You can change the default folder at any time using the ESM Console.

For more information, see Forensics Flow.
You can deploy the Traps solution in a wide range of environments. The following topics describe typical deployment scenarios that take into account the number of agents and sites:

- Standalone Deployment
- Small Deployments
- Large Deployments

For installation prerequisites and considerations, see Prerequisites.
Standalone Deployment

For an initial proof of concept (POC) or a small site with fewer than 3000 Traps agents, use a standalone deployment to install the following Endpoint Security Manager (ESM) components on a single server or virtual machine:

- ESM Server
- ESM Console
- Forensic (quarantine) folder
- Database
- *(Recommended)* WildFire integration
- *(Optional)* Load balancer for distributing traffic across ESM Servers
- *(Optional)* External logging platform, such as an SIEM or syslog

For best practices on using a phased approach for installing Traps on endpoints, see Recommended Traps Deployment Process.
Small Deployments

- Small Single-Site Deployment
- Small Multi-Site Deployment

Small Single-Site Deployment

This deployment scenario supports up to 16,000 Traps agents in a single-site environment and consists of the following components:

- One dedicated database server
- One ESM Console for managing the security policy and Traps agents
- Two ESM Servers, one primary and one backup, on the same network segment as the database server and ESM Console
- One forensic folder accessible by all endpoints for storing real-time forensic details about security events
- *(Recommended)* WildFire integration
- *(Optional)* Load balancer for distributing traffic across ESM Servers
- *(Optional)* External logging platform, such as an SIEM or syslog

In this deployment scenario, a single site contains the database, ESM Console for managing local policies and endpoints, and redundant ESM Servers. In the event that the primary ESM Server is inaccessible, Traps agents connect to the Endpoint Security Manager using the backup server. Both servers obtain the security policy from the database and distribute the policy to the agents.
Small Multi-Site Deployment

This deployment scenario supports up to 32,000 Traps agents in a multi-site environment and consists of the following components:

- One dedicated database server at one of the sites
- One ESM Console in the same location as the database for managing the security policy and Traps agents
- One ESM Server per site or two ESM Servers per site for redundancy
- One forensic folder accessible by all endpoints for storing real-time forensic details about security events
- *(Recommended)* WildFire integration
- *(Optional)* Load balancer for distributing traffic across ESM Servers
- *(Optional)* External logging platform, such as an SIEM or syslog

In this deployment scenario, Site A contains an ESM Server, database, and ESM Console for managing local policies and endpoints. Site B contains a second ESM Server that is capable of supporting up to 16,000 additional agents (32,000 Traps agents total). Both servers obtain the security policy from the database located in Site A and distribute the policy to the agents. The agents connect to the primary ESM Server on their site while the ESM Server in the other site acts as a secondary backup server.
Large Deployments

- Large Single-Site Deployment
- Large Multi-Site Deployment with One Endpoint Security Manager
- Large Multi-Site Deployment with Roaming Agents (Without VPN)
- Large Multi-Site Deployment with Roaming Agents (With VPN)

Large Single-Site Deployment

This deployment scenario supports up to 80,000 Traps agents in a single-site environment and consists of the following components:

- One dedicated database server
- One ESM Console in the same location as the database for managing the security policy and Traps agents
- One ESM Server for every 16,000 Traps agents
- One forensic folder for each ESM Server that is accessible by all endpoints for storing real-time forensic details about security events
- (Recommended) WildFire integration
- (Optional) Load balancer for distributing traffic across ESM Servers
- (Optional) External logging platform such as an SIEM or syslog

In this example, up to 80,000 Traps agents can connect to the Endpoint Security Manager. To support this scenario, the endpoints connect to five ESM Servers through an optional load balancer. Each ESM Server connects to a central database that is managed by a dedicated ESM Console.
Large Multi-Site Deployment with One Endpoint Security Manager

This deployment scenario supports up to 80,000 Traps agents in a multi-site environment that consists of the following components:

- One dedicated database server
- One ESM Console in the same location as the database for managing the security policy and Traps agents
- One ESM Server for every 16,000 Traps agents
- One forensic folder for each ESM Server that is accessible by all endpoints for storing real-time forensic details about security events
- (Recommended) WildFire integration
- (Optional) Load balancer for distributing traffic across ESM Servers
- (Optional) External logging platform such as an SIEM or syslog

In this example, Sites A, B, C, D, and E each need to support up to 16,000 Traps agents. To support this scenario, you must deploy an ESM Server in each site that retrieves the security policy from the database located in Site A. The agents connect to the Endpoint Security Manager using their local ESM Servers as the primary server and use the ESM Servers at other sites as secondary servers.
Large Multi-Site Deployment with Roaming Agents (Without VPN)

This deployment scenario supports up to 80,000 Traps agents in a multi-site environment and consists of the following components:

- One dedicated database server
- One ESM Console in the same location as the database for managing the security policy and Traps agents
- One ESM Server for every 16,000 Traps agents in each site
- One ESM Server with a public-facing DNS record that accepts connections from roaming Traps agents configured in one of two ways:
  - Configured with a port that accepts connections from external networks
  - Installed in a DMZ with a connection to the internal database server
  
  *This server can also function as a backup server.*

- One forensic folder for each ESM Server that is accessible by all endpoints for storing real-time forensic details about security events
- *(Recommended)* WildFire integration
- *(Optional)* Load balancer for distributing traffic across ESM Servers
- *(Optional)* External logging platform such as an SIEM or syslog

In this example, Sites A, B, C, and D each need to support up to 16,000 Traps agents. An additional site supports up to 16,000 Traps agents that are roaming. To support this scenario, each site contains an ESM Server that retrieves the security policy from the database located at Site A. Internal endpoints connect to the Endpoint Security Manager using their local ESM Servers. External endpoints connect through a publicly available ESM Server located in a DMZ or through a port that is configured to allow traffic from external networks. If an endpoint is roaming and cannot connect to the ESM Server, Traps collects prevention data locally until the agent can establish a connection to the forensic folder.
Large Multi-Site Deployment with Roaming Agents (With VPN)

This deployment scenario supports up to 48,000 Traps agents that can connect through local sites and from off-site locations through a VPN tunnel (to support up to 80,000 Traps agents, you can deploy two additional ESM sites). This multi-site environment consists of the following components:

- One dedicated database server
- One ESM Console in the same location as the database for managing the security policy and Traps agents
- One ESM Server for every 16,000 Traps agents in each site
- GlobalProtect or an alternative VPN gateway to provide roaming users with an internal IP address for accessing the ESM Server
- One forensic folder for each ESM Server that is accessible by all endpoints for storing real-time forensic details about security events
- (Recommended) WildFire integration
- (Optional) Load balancer for distributing traffic across ESM Servers
- (Optional) External logging platform such as an SIEM or syslog

In this example, Sites A, B, and C each need to support up to 16,000 Traps agents with some of those agents located off-site. To support this scenario, each site contains an ESM Server that retrieves the security policy from the database located at Site A. Internal endpoints connect to the Endpoint Security Manager using their local ESM Servers. External endpoints connect through a VPN tunnel that provides...
the endpoint with an internal IP address for connecting to the site. If an endpoint is roaming and cannot connect over VPN, Traps collects prevention data locally until the agent can establish a connection to the forensic folder.
Prerequisites

The following topics describe prerequisites for installing the Traps infrastructure:

> Hardware Requirements
> Software Requirements
Hardware Requirements

- Standalone Endpoint Security Manager Hardware Requirements
- Distributed Endpoint Security Manager Hardware Requirements
- Traps Hardware Requirements

Standalone Endpoint Security Manager Hardware Requirements

In a **Standalone Deployment**, you install the Endpoint Security Manager components—which consists of the ESM Server, ESM Console, and database—on the same server. The following table displays the hardware requirements for the standalone server.

<table>
<thead>
<tr>
<th>Specification</th>
<th>250 Agents</th>
<th>3000 Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2-Core Intel Xeon E5-2660 V2</td>
<td>4-Core Intel Xeon E5-2660 V2</td>
</tr>
<tr>
<td></td>
<td>2.2GHz or better</td>
<td>2.2GHz or better</td>
</tr>
<tr>
<td>Disk space for Traps</td>
<td>• First year: 250MB</td>
<td>• First year: 2.5GB</td>
</tr>
<tr>
<td>data</td>
<td>• Second year: 500MB</td>
<td>• Second year: 5GB</td>
</tr>
<tr>
<td></td>
<td>• Third year: 1GB</td>
<td>• Third year: 10GB</td>
</tr>
<tr>
<td>RAM</td>
<td>4GB</td>
<td>16GB</td>
</tr>
<tr>
<td>Database</td>
<td>SQL Express</td>
<td>SQL Server</td>
</tr>
</tbody>
</table>

For Traps requirements, see [Traps Hardware Requirements](#).

Distributed Endpoint Security Manager Hardware Requirements

In a distributed deployment, you install the Endpoint Security Manager components—which consists of the ESM Server, ESM Console, and database—on different servers.
The following table displays the hardware requirements for each Endpoint Security Manager. For hardware requirements to install the ESM components on a standalone server, see Standalone Endpoint Security Manager Hardware Requirements.

<table>
<thead>
<tr>
<th>Specification</th>
<th>500 Agents</th>
<th>5,000 Agents</th>
<th>10,000 Agents</th>
<th>16,000 Agents</th>
<th>50,000 Agents</th>
<th>80,000 Agents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESM Console Hardware Requirements</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>2-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
</tr>
<tr>
<td><strong>Disk space</strong></td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>4GB</td>
<td>8GB</td>
<td>8GB</td>
<td>8GB</td>
<td>8GB</td>
<td>8GB</td>
</tr>
<tr>
<td><strong>ESM Server Hardware Requirements</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>2-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>Install 4 or more ESM Servers to support this number of agents (each server supports up to 16,000 agents)</td>
<td>Install 5 ESM Servers to support this number of agents (each server supports up to 16,000 agents)</td>
</tr>
<tr>
<td><strong>Disk space</strong></td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td>3GB plus 50GB for the forensic folder</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RAM</strong></td>
<td>4GB</td>
<td>4GB</td>
<td>8GB</td>
<td>8GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Database Hardware Requirements</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>4-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
<td>8-Core Intel Xeon E5-2660 V2 2.2GHz or better</td>
</tr>
<tr>
<td><strong>Disk space for Traps data</strong></td>
<td>• First year: 250MB</td>
<td>• First year: 2.5GB</td>
<td>• First year: 7.5GB</td>
<td>• First year: 26GB</td>
<td>• First year: 52GB</td>
<td>• First year: 104GB</td>
</tr>
<tr>
<td>Specification</td>
<td>500 Agents</td>
<td>5,000 Agents</td>
<td>10,000 Agents</td>
<td>16,000 Agents</td>
<td>50,000 Agents</td>
<td>80,000 Agents</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Processor</td>
<td>Third year: 1GB</td>
<td>Third year: 10GB</td>
<td>Third year: 20GB</td>
<td>Third year: 30GB</td>
<td>Third year: 100GB</td>
<td>Third year: 200GB</td>
</tr>
<tr>
<td>RAM</td>
<td>4GB RAM</td>
<td>8GB RAM</td>
<td>8GB RAM</td>
<td>8GB RAM</td>
<td>32GB RAM</td>
<td>32GB RAM</td>
</tr>
</tbody>
</table>

Also see [Traps Hardware Requirements](#).

### Traps Hardware Requirements

The following table displays the hardware requirements for each endpoint.

<table>
<thead>
<tr>
<th>Specification</th>
<th>Per Endpoint</th>
</tr>
</thead>
</table>
| Processor     | Intel Pentium 4 or later with SSE2 instruction set support  
|               | AMD Opteron/Athlon 64 or later with SSE2 instruction set support |
| Disk space    | 200MB minimum; 20GB recommended |
| RAM           | 512MB minimum; 2GB recommended |

For software requirements see [Traps Software Requirements](#).
Software Requirements

- ESM Console Software Requirements
- ESM Server Software Requirements
- Database Software Requirements
- Traps Software Requirements

ESM Console Software Requirements

Before installing ESM Console software, make sure that the server meets the following prerequisites:

- ESM Server and ESM Console are running the same version
- ESM Console hostname of 15 or fewer characters
- English-language version of a physical or virtual Windows Server. To determine which versions of Windows Server are supported, refer to Where Can I Install the Endpoint Security Manager (ESM)? in the Palo Alto Networks® Compatibility Matrix.
- Internet Information Services (IIS) 7.0 or above with ASP.NET and Static Content Compressions components
- .NET Framework 4.5.1 Full
- SSL certificate from a trusted certificate authority (CA) with server authentication and client authentication (recommended)
- Allow communication on the TCP port from clients to server (the default is port 2125)
- Forensic folder with BITS enabled
- Allow communication on HTTP port (80) or HTTPS port (443) from the clients to the quarantine folder
- Browser, any of the following:
  - Internet Explorer 10 and later versions
  - Microsoft Edge (all versions)
  - Chrome 30 and later versions
  - Firefox 35 and later versions
  - Opera 25 and later versions
- ESM Console Hardware Requirements

ESM Server Software Requirements

Each ESM Server supports up to 16,000 Traps agents. In a multi-ESM deployment, you can deploy a maximum of five ESM Servers to support a total of 80,000 agents.

Before installing ESM Server software, make sure that the server meets the following prerequisites:

- ESM Server and ESM Console running the same version.
- ESM Server hostname of 15 or fewer characters
- Ensure that the round-trip communication time between the ESM Server and the database is less than 80 ms.
- .NET Framework 4.5.1 Full
- SSL certificate from a trusted certificate authority (CA) with server authentication and client authentication (recommended)
- Allow communication on the TCP port from clients to server (the default is port 2125)
- Forensic folder with BITS enabled
- Internet Information Services (IIS) 7.0 or above with ASP.NET and Static Content Compressions components
English-language version of a physical or virtual Windows Server. To determine which versions of Windows Server are supported, refer to Where Can I Install the Endpoint Security Manager (ESM)? in the Palo Alto Networks® Compatibility Matrix.

Communication between the ESM Server and the agents is based on Windows Communication Foundation (WCF) client with version TLS/SSL 1.0.

ESM Server Hardware Requirements

Database Software Requirements

The server-side applications require an SQL database that can be either a local database installed on the same server as the ESM Console or ESM Server, or an external database installed on another machine. If you plan to deploy multiple ESM Servers, install the database on the ESM Console or use an external database.

Consult with the Palo Alto Networks support team if you require integration with an existing database.

Provision a database server that meets the following prerequisites:

- Database application for use during evaluation or production. Use one of the following:

<table>
<thead>
<tr>
<th>Versions</th>
<th>SQL Server Express</th>
<th>SQL Server Enterprise</th>
<th>SQL Server Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• 2008 R2</td>
<td>• 2008 R2</td>
<td>• 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• 2012</td>
<td>• 2012</td>
<td>• 2012</td>
</tr>
<tr>
<td></td>
<td>• 2014</td>
<td>• 2014</td>
<td>• 2014</td>
</tr>
<tr>
<td></td>
<td>• 2016</td>
<td>• 2016</td>
<td>• 2016</td>
</tr>
<tr>
<td></td>
<td>2012 with Always On*</td>
<td>2012 with Always On*</td>
<td>2012 with Always On*</td>
</tr>
<tr>
<td></td>
<td>2014 with Always On*</td>
<td>2014 with Always On*</td>
<td>2014 with Always On*</td>
</tr>
<tr>
<td></td>
<td>2016</td>
<td>2016</td>
<td>2016</td>
</tr>
<tr>
<td></td>
<td>2016 with Always On*</td>
<td>2016 with Always On*</td>
<td>2016 with Always On*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Always On based on group availability</td>
<td></td>
</tr>
</tbody>
</table>

- Agents supported during evaluation

|                               | • 200 endpoints | • 200 endpoints | • 200 endpoints |
|                               | • 50 VDI        | • 50 VDI        | • 50 VDI        |
|                               | • 50 server     | • 50 server     | • 50 server     |

- Agents supported during production

|                               | 250               | 80,000 per database cluster | 80,000 per database cluster |

Agents supported during evaluation

Agents supported during production

Traps Software Requirements

Before installing Traps software, make sure that the target endpoint meets the following prerequisites:

- ESM Server and ESM Console running the same or a later version than the Traps agent
Operating system: Palo Alto Networks supports Traps on many Windows operating systems. To determine the minimum Traps release for a specific operating system, refer to Where Can I Install the Traps Agent? in the Palo Alto Networks® Compatibility Matrix.

Virtual Environments:
- VMware ESX
- Citrix XenServer
- Oracle Virtualbox
- Microsoft Hyper-V

Virtual Desktop Infrastructure (VDI):
- VMware Horizon View
- Citrix XenDesktop

.NET:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>.NET Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 and earlier releases</td>
<td>.NET 3.5 SP1 or 3.5.1</td>
</tr>
<tr>
<td>Windows 8</td>
<td>.NET 4.5</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>.NET 4.5.1</td>
</tr>
<tr>
<td>Windows 10 and later releases</td>
<td>.NET 4.6</td>
</tr>
<tr>
<td>Windows Server 2008</td>
<td>.NET 3.5 SP1 or 3.5.1</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>.NET 4.5</td>
</tr>
<tr>
<td>Windows Server 2012 R2 and later releases</td>
<td>.NET 4.5.1</td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>.NET 4.5.1</td>
</tr>
</tbody>
</table>

Allow communication on the TCP port from clients to server (the default is port 2125)

BITS client

Windows Accessories (Notepad) to view logs

Windows Event Log service

Traps Hardware Requirements
Set Up the Traps Infrastructure

The following topics describe how to set up the Traps infrastructure components:

- Set Up the Endpoint Infrastructure
- Set Up the Endpoint Security Manager
- Set Up the Endpoints
- Install Traps Components Using Msiexec
- Verify a Successful Installation
Set Up the Endpoint Infrastructure

Use the following workflow to set up the Endpoint infrastructure or, to upgrade your existing Endpoint infrastructure, use the workflow to Upgrade to Traps 3.4 described in the Traps 3.4 New Features Guide:

STEP 1 | Review the installation considerations of the software.
   Endpoint Infrastructure Installation Considerations
   Prerequisites

STEP 2 | Review the recommended implementation stages.
   Recommended Traps Deployment Process

STEP 3 | (Optional) Configure SSL encryption.
   TLS/SSL Encryption for Traps Components

STEP 4 | (Optional) Configure the MS-SQL Server.
   Database Software Requirements
   Configure the MS-SQL Server Database

STEP 5 | Install the ESM Server software.
   ESM Server Software Requirements
   Install the Endpoint Security Manager Server Software
   (Optional) Install Traps Components Using Msiexec

STEP 6 | Install the ESM Console software.
   ESM Console Software Requirements
   Install the Endpoint Security Manager Console Software
   (Optional) Install Traps Components Using Msiexec

STEP 7 | Install the Traps agent on the endpoints.
   Traps Software Requirements
   Install Traps on Windows Endpoints
   (Optional) Install Traps Components Using Msiexec

STEP 8 | Verify the installation is successful.
   Verify a Successful Installation
Set Up the Endpoint Security Manager

- Endpoint Infrastructure Installation Considerations
- TLS/SSL Encryption for Traps Components
- Configure the MS-SQL Server Database
- Install the Endpoint Security Manager Server Software
- Install the Endpoint Security Manager Console Software

Endpoint Infrastructure Installation Considerations

To install or upgrade the ESM components consider the following:

- The ESM Server and the ESM Console must run the same version.
- The ESM Server and the ESM Console support mixed versions of Traps and are also backward compatible with earlier versions. For example, an ESM Server and ESM Console can support a mix of Traps agents running both the current release and the previous release.

Also see: Prerequisites.

TLS/SSL Encryption for Traps Components

The Endpoint Security Manager supports Transport Layer Security (TLS) versions 1.0 and Secure Sockets Layer (SSL) version 3.0. TLS/SSL, which is often referred to simply as SSL, enables clients to trust the identity of the server and the transmission of data. Traps components use SSL to secure communication by encrypting:

- Traffic between the ESM Server and the Traps agents
- Traffic between the administrative user and the ESM Console
- Traffic between the ESM Server and WildFire
- BITS protocol used to transfer data between the agent and the forensics folder

Enabling SSL for Traps components is a three step-process: First, you must request or issue a certificate for each ESM Server and ESM Console. Note that traffic between the ESM Server and WildFire does not require any additional configuration as the ESM Server encrypts traffic using the default trusted third-party certificates that comes with Windows. Next, you enable SSL encryption during the installation of the ESM Server and ESM Console. Finally, depending on the type of certificate, you deploy the certificate to your endpoints. For detailed instructions, see the following workflow:

STEP 1 | Request or generate a certificate for each ESM component—server and console—with a purpose of server and client authentication. This certificate must be one that you can export with a password.

The certificate can have a single name or a wildcard name. A single-name certificate requires the Common Name (CN) of the certificate to match the fully qualified domain name (FQDN) of the ESM component (for example, server.trapsserver.com). A wildcard-name certificate enables you to use the same certificate for multiple ESM components that share the same sub-domain (for example, *.trapsserver.com can be used for both server.trapsserver.com and console.trapsserver.com). Wildcard-name certificates are also useful in deployments that use multiple ESM Servers.

If you use a wildcard-name certificate, it is recommended to configure the server name using the FQDN when installing the ESM software.

Use one of the following basic approaches to obtain certificates:
• **Obtain a certificate from a trusted-party CA**—The benefit of obtaining a certificate from a trusted third-party certificate authority (CA), such as GoDaddy, is that the endpoint will already trust the certificate because Windows updates and common browsers include root CA certificates from well-known CAs in their trusted root certificate stores.

• **Obtain certificates from an enterprise CA**—Enterprises that have their own internal root CA can use it to issue certificates for ESM components. The benefit is that domain-joined clients probably already trust the enterprise CA. Another benefit of this method is that the private key does not leave the ESM component.

• **Generate self-signed certificates**—A self-signed certificate is a certificate that is signed by the same entity whose identity it certifies. You can use IIS Manager or any other publicly available tool to generate a self-signed certificate and then deploy it to the endpoint.

**STEP 2 | Install the ESM software and enable SSL encryption (for full installation instructions, see Install the Endpoint Security Manager Server Software and Install the Endpoint Security Manager Console Software).**

1. During the installation of both the ESM Server and ESM Console, select the **External Certificate (SSL)** option and browse to the PKCS#12 or PFX file containing the certificate and private key.

   *If you do not already have a PKCS#12 or PFX file, use your preferred method to generate it. For example, to do this in IIS, you can use the Export function in the MMC Console > Certificates snap-in. When you export the certificate and private key, it is required to set a password to protect the private key.*

2. Enter the certificate password.

   The installer binds the certificate to the selected agent-ESM communication port.

   If you install Traps on the ESM Server and ESM Console, and use either a self-signed or an enterprise CA certificate, you must also install the certificate on the server as described in the following step.

**STEP 3 | (Certificates issued by an enterprise CA and self-signed certificates) Install the certificate in the trusted root certificate store (CA certificates and self-signed certificates) of the computer account. Certificates issued by a trusted third-party CA are automatically trusted by the endpoint due to the chain of trust and do not require installation.**

1. Add the certificate to the endpoint using one of the following methods:
   - Copy the certificates manually.
   - Include the certificate in the master image for new endpoints.
   - Use a centralized deployment method such as an Active Directory Group Policy Object (GPO).
2. Verify that the certificate appears in the appropriate store on the endpoint.

**Configure the MS-SQL Server Database**

The Endpoint Security Manager requires a database that is managed over the SQL Server platform (for supported SQL Server versions, see Database Software Requirements). The Endpoint Security Manager uses the database to store administrative information, security policy rules, information about security events, and other information.

Before installing the Endpoint Security Manager, configure the SQL database with the required permissions. When using Windows Authentication as the user authentication method, the owner must have rights to *Log on as a service* and be a local administrator on the ESM Server.

The following procedure is recommended as a best practice for creating and configuring the MS-SQL Server database.
STEP 1 | Create a new database.
   1. Select SQL Server Management Studio from the Start menu.
   2. Click Connect to open Microsoft SQL Server Management Studio.

   ![SQL Server Management Studio](image)

   3. Right-click Databases and then select New Database.

STEP 2 | Configure the database settings.
   The database owner that you specify must already exist as a local or domain administrator.

   ![New Database](image)

   1. Enter the Database name.
   2. Select the database Owner:
      1. Click the ellipsis (…) button.
      2. Enter the object name in the format [domain\user] or Browse to an object name.
      3. Select Check Names to validate the database owner.
   3. Click OK and then click OK again.

STEP 3 | Verify the database owner privileges.
   1. Expand the database you created and then select Security > Users.
   2. Double-click dbo.
3. Select the Owned Schemas page and then select db_owner.
4. Select the Membership page and then select db_owner.
5. Click OK.

Install the Endpoint Security Manager Server Software

Before installing the Endpoint Security Manager (ESM) Server software, verify that the system meets the requirements described in ESM Server Software Requirements.

STEP 1 | Before you begin:
- Verify that the system meets the requirements described in ESM Server Software Requirements.
- Obtain the software and license file from your Palo Alto Networks Account Manager, reseller, or from https://support.paloaltonetworks.com.
- If you are using Windows authentication to authenticate with the database, you must add the database owner account as a local administrator on the ESM Server (for more information, see Configure the MS-SQL Server Database).

STEP 2 | Initiate the ESM Server software installation. You can also install the ESM Server using Msiexec (see Install Traps Components Using Msiexec).
1. Double click the ESMCore installation file.
2. Click Next to begin the setup process.
3. On the End User License Agreement dialog, select the I accept the terms in the License Agreement check box and then click Next.
4. Keep the default installation folder or click Change to specify a different installation folder and then click Next.

STEP 3 | Configure the settings that enable communication between the ESM Server and the database.
To set up access to the database, you must specify the authentication method and a user that has administrative privileges to administer the database. The username (and password) that you enter depend on the type of authentication method that you select: either Windows authentication (recommended) or SQL server authentication.
1. Select the type of database that you installed for use with the Endpoint Security Manager.
2. Enter the fully qualified domain name or IP address of the database Server Name.
3. Enter the name of the Database. If your SQL Server uses an instance other than the default, you must also include the instance name in the format `<instance>/<databasename>`.
4. Select the method of authentication and enter the account credentials for the database owner.
   - **Use Windows Authentication** to authenticate using a Windows domain user account that has privileges to connect to the database server and enter the Domain\User (for example, `mydomain\administrator`) and Password. This account must also be added as a local administrator on the ESM Server.
   - **Use SQL Server Authentication** to authenticate using a local user that has privileges to administer the database and enter the Login and Password.
5. Click Next.

**STEP 4 | Specify the security level for communication between the ESM Server and the Traps agents.**

To encrypt communication over SSL, use a server-client certificate file (PFX format) and supply the password for decrypting the private key.

1. Select the certificate configuration method:
   - **Select External Certificate (SSL)**—Encrypt communication between the server and the agents over SSL (default). Then browse to the server-client certificate and enter the password required to decrypt the private key.
   - **No Certificate (no SSL)**—Do not encrypt communication between the server and the agents (not recommended).
2. Click Next.

**STEP 5 | Configure the settings for the administrative user.**
1. Choose the type of authentication you want to use:
   - **Machine**—The Endpoint Security Manager authenticates using users and groups on the local machine.
   - **Domain**—The Endpoint Security Manager authenticates using users and groups belonging to the domain of the machine.
2. Enter the account name for the user who will administer the server in the **Please specify an administrative user** field and then click **Next**.

**STEP 6** | Configure additional settings for your ESM Server.

1. Specify the **ESM Server port** to use for access to the server or keep the default setting (2125).
2. Enter and then confirm an uninstall password, which must be eight characters or more. You will be prompted for this password any time you try to uninstall ESM or Traps software.

   After installing the ESM Server software, you can **Change the Uninstall Password at a later date by creating an agent settings rule using the ESM Console**.
3. Click **Next**.

**STEP 7** | Import a license.
1. **Browse** to the license file and then click **Open**. If you do not have a license, contact your Account Manager, reseller, or go to https://support.paloaltonetworks.com.

   The installer displays license details for the license file.

2. Click **Next**.

**STEP 8 | Complete the installation.**

1. Click **Install**.
2. When the installation is complete, click **Finish**.

---

### Install the Endpoint Security Manager Console Software

You can install the ESM Console software on a dedicated server or on the same server as the ESM Server software. Each ESM Console requires a dedicated license.

**STEP 1 | Before you begin:**

- Verify that the system meets the requirements described in **ESM Console Software Requirements**.
- Obtain the software from your Palo Alto Networks Account Manager, reseller, or from https://support.paloaltonetworks.com.

**STEP 2 | Initiate the ESM Console software installation.** You can also install the ESM Console using Msiexec (see **Install Traps Components Using Msiexec**).

1. Double click the **ESMConsole** installation file.
2. Click **Next** to begin the setup process.
3. Select the **I accept the terms of the License Agreement** check box and then click **Next**.

**STEP 3 | Specify the installation folder for the ESM Console.**

Keep the default installation folder or click **Change** to specify a different installation folder and then click **Next**.

**STEP 4 | Configure the settings that enable communication between the ESM Console and the database.**

To set up access to the database, you must specify the authentication method and a user that has administrative privileges to administer the database. The username (and password) that you enter depend on the type of authentication method that you select: either Windows authentication (recommended) or SQL server authentication.
Use the same database settings that you entered during the ESM Server installation.

1. Select the type of database that you installed for use with the ESM Server.
2. Enter the fully qualified domain name or IP address of the database Server Name.
3. Enter the name of the Database. If your SQL Server uses an instance other than the default, you must also include the instance name in the format <instance>/<databasename>.
4. Select the method of authentication and enter the account credentials:
   - Use Windows Authentication to authenticate using a Windows domain user account that has privileges to connect to the database server and enter the Domain\User (for example, mydomain\administrator) and Password.
   - Use SQL Server Authentication to authenticate using a local user that has privileges to administer the database and enter the Login and Password.
5. Click Next.

STEP 5 | Specify the security level for communication between the administrator and the ESM Console.
To encrypt communication over SSL, use a server-client certificate file (PFX format) and supply the password for decrypting the private key.

1. Select the certificate configuration method:
   - Select External Certificate (SSL)—(Recommended) Encrypt communication to and from the ESM Console over SSL (default). Then browse to the server-client certificate and enter the password required to decrypt the private key.
   - No Certificate (no SSL)—Do not encrypt communication to and from the ESM Console.
2. Click Next.

STEP 6 | Specify the forensic folder.
1. Keep the default forensic folder path or **Browse** to an alternate folder location and click **OK**.

   The installer automatically enables BITS for this folder.

2. Click **Next**.

**STEP 7 | Complete the installation.**

1. Click **Install**.
2. When the installation is complete, click **Finish**.
Set Up the Endpoints

To set up Traps on the endpoints within your organization, see the following topics:

- Recommended Traps Deployment Process
- Traps Installation Options
- Install Traps on Windows Endpoints

Recommended Traps Deployment Process

The Traps software is typically deployed to endpoints across a network after an initial proof of concept (POC), which simulates the corporate production environment. During the POC or deployment stage, you analyze security events to determine which are triggered by malicious activity and which are due to legitimate processes behaving in a risky or incorrect manner. You also simulate the number and types of endpoints, the user profiles, and the types of applications that run on the endpoints in your organization and, according to these factors, you define, test, and adjust the organization’s security policy.

The goal of this multi-step process is to provide maximum protection to the organization without interfering with legitimate workflows.

After the successful completion of the initial POC, we recommend a multi-step implementation in the corporate production environment for the following reasons:

- The POC doesn't always reflect all the variables that exist in your production environment.
- There is a rare chance that the Traps agent will affect business applications, which can reveal vulnerabilities in the software as a prevented attack.
- During the POC, it is much easier to isolate issues that appear and provide a solution before full implementation in a large environment where issues could potentially affect a large number of users.

A multi-step deployment approach ensures a smooth implementation and deployment of the Traps solution throughout your network. Use the following steps for better support and control over the added protection.

<table>
<thead>
<tr>
<th>Step</th>
<th>Duration</th>
<th>Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install Traps on endpoints.</td>
<td>1 week</td>
<td>Install the Endpoint Security Manager (ESM), including an MS SQL database, ESM Console, and ESM Server, and install the Traps agent on a small number of endpoints (3 to 10). Test normal behavior of the Traps agents (injection and policy) and confirm that there is no change in the user experience.</td>
</tr>
<tr>
<td>2. Expand the Traps deployment.</td>
<td>2 weeks</td>
<td>Gradually expand agent distribution to larger groups that have similar attributes (hardware, software, and users). At the end of two weeks you can have Traps deployed on up to 100 endpoints.</td>
</tr>
<tr>
<td>3. Complete the Traps installation.</td>
<td>2 or more weeks</td>
<td>Broadly distribute the Traps agent throughout the organization until all endpoints are protected.</td>
</tr>
<tr>
<td>4. Define corporate policy and protected processes.</td>
<td>Up to 1 week</td>
<td>Add protection rules for third-party or in-house applications and then test them.</td>
</tr>
</tbody>
</table>
### Traps Installation Options

You can install Traps in the following ways:

- **Install from the endpoint**—In situations where you need to install Traps on a small number of endpoints, you can manually install the Traps software using the workflow described in Install Traps on Windows Endpoints.

- **Install using Msiexec**—To install Traps from the command line, use the Msiexec utility to perform operations on a Windows Installer as described in Install Traps Components Using Msiexec. You can also use the Msiexec installation options with MSI deployment software such as a Policy System Center Configuration Manager (SCCM), Altiris, or Group Policy Object (GPO). Using MSI deployment software is recommended to install Traps across an organization or a large number of endpoints.

- **Install using an action rule**—If the endpoints in your organization already have Traps installed, you can upgrade the Traps software by configuring an action rule as described in Uninstall or Upgrade Traps on the Endpoint.

### Install Traps on Windows Endpoints

Before installing Traps, verify that the system meets the requirements described in Traps Software Requirements.

**STEP 1** | Initiate the Traps software installation. You can also install Traps using Msiexec (see Install Traps Components Using Msiexec).

> The version(s) of Traps that you install on your endpoints must be the same as or older than the ESM Server and ESM Console version.

1. Obtain the software from your Palo Alto Networks Account Manager, reseller, or from https://support.paloaltonetworks.com.
2. Unzip the zip file and double click the **Traps** installation file; choose either the x64 (64-bit) or x86 (32-bit) version depending on your endpoint’s OS.
3. Click **Next**.
4. Select **I accept the terms in the License Agreement** and then click **Next**.

**STEP 2** | Configure the Traps agents to connect to the ESM Server.

1. Provide the following information for the ESM Server:
   - **Host Name**—Enter the FQDN or IP address of the ESM Server.
   - **Port**—Change the port number, if required (default is 2125).
   - **Use**—Select **SSL** to encrypt communication to the server (default) or **No SSL** to not encrypt communication (not recommended).
2. Click **Next > Install**.
We recommend that you restart the endpoint after completing the installation.
Install Traps Components Using Msiexec

As an alternative to using the installation files, you can use Windows Msiexec to install software for the following Traps components: the ESM Server, the ESM Console, and the Traps agent. Msiexec provides full control over the installation process and allows you to install, modify, and perform operations on a Windows Installer from the command line interface (CLI). You can also use MSIXEC to log any issues encountered during installation.

Additionally, to install Traps on multiple endpoints for the first time, you can use Msiexec in conjunction with a System Center Configuration Manager (SCCM), Altiris, Group Policy Object (GPO), or other MSI deployment software. After successfully installing Traps on an endpoint and establishing an initial connection with the ESM Server, you can upgrade or uninstall Traps from one or more endpoints by creating an action rule (see Uninstall or Upgrade Traps on the Endpoint).

Before installing Traps, verify that the system meets the requirements described in Traps Software Requirements.

- Install Traps Components
- Uninstall Traps Components

Install Traps Components

Use the following workflow to install Traps components (the ESM Server, the ESM Console, and the Traps agent) using Msiexec.

**STEP 1** | Open a command prompt as an administrator:

- Select Start > All Programs > Accessories. Right-click Command prompt, and then Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

**STEP 2** | Run the msiexec command followed by one or more of the following options or properties:

- Install, display, and logging options:
  - /i <installpath>\<installerfilename>.msi—Install a package. For example, msiexec /i c:\install\traps.msi.
  - /qn—Displays no user interface (quiet installation). At minimum, you must also specify the host server name or IP address using the CYVERA_SERVER property.
  - /L*v <logpath>\<logfile>.txt—Log verbose output to a file. For example, /L*v c:\logs\install.txt.

For a full list of Msiexec parameters, see https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/msiexec.mspx

- Public properties:
  - CYVERA_SERVER=<servername>—Primary host server name or IP address (default is ESMserver)
  - CYVERA_SERVER_PORT=<serverport>—Primary host server port (default is 2125)
  - USE_SSL_PRIMARY=[0 | 1]—(Quiet installation only) Set encryption preferences on the primary server by specifying 0 to not use SSL (not recommended) or 1 to use SSL (default)

For example, to install Traps without a user interface, specify a server named TrapsServer that does not use SSL encryption on a port other than the default (for example on port 5212, a non-standard port), and create an installation log in C:\temp, enter the following:
msiexec /i c:\install\traps.msi /qn CYVERA_SERVER=TrapsServer
USE_SSL_PRIMARY=0 CYVERA_SERVER_PORT=5212 /I\v C:\temp\trapsinstall.log

We recommend that you restart the device after completing the installation.

Uninstall Traps Components

Use the following workflow to uninstall Traps components (the ESM Server, the ESM Console, and the Traps agent) using Msiexec.

**STEP 1** | Open a command prompt as an administrator:
- Select Start > All Programs > Accessories. Right-click Command prompt, and then Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

**STEP 2** | Run the msiexec command followed by one or more of the following options or properties:
- Uninstall and logging options:
  - /x <installpath>\<installerfilename>.msi—Uninstall a package. For example, msiexec /x c:\install\traps.msi.
  - /L*v <logpath>\<logfile>.txt—Log verbose output to a file. For example, /L*v c:\logs\uninstall.txt.

For a full list of Msiexec parameters, see https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/msiexec.mspx

- Public properties:
  - UNINSTALL_PASSWORD=<uninstallpassword>—Specify the administrator password.

To uninstall Traps and log verbose output to a file called uninstallLogFile.txt, enter the following command:

msiexec /x c:\install\traps.msi UNINSTALL_PASSWORD=[palo@lt0] /I\v c:\install\uninstallLogFile.txt

You must specify the UNINSTALL_PASSWORD property to successfully uninstall a package.
Verify a Successful Installation

You can verify the success of the ESM server and endpoint installations by verifying connectivity between the server and each endpoint from both sides of the connection.

- Verify Connectivity from the Endpoint
- Verify Connectivity from the ESM Console

Verify Connectivity from the Endpoint

After successfully installing Traps, the Traps agent should be able to connect to the server that is running the Endpoint Security Manager.

**STEP 1** | Launch the Traps Console from the taskbar:

- From the Windows taskbar, double-click the Traps icon (or right-click the icon and select **Console**).
- Run CyveraConsole.exe from the Traps installation folder.

**STEP 2** | Verify the status of the server connection. If Traps is connected to the server, the **Connection** status reports that the connection is successful. If the Traps agent is unable to establish a connection with the primary or secondary server, the Traps Console reports a disconnected status.

[Image of Traps Console]

**STEP 3** | Verify Connectivity from the ESM Console.

Verify Connectivity from the ESM Console

After successfully verifying that the endpoint can reach the ESM Server, verify that the endpoint appears in the list of computers on the **Monitor > Agent > Health** page of the ESM Console.

[Image of ESM Console]

**STEP 1** | From the ESM Console, select **Monitor > Agent > Health**.

**STEP 2** | Locate the name of the endpoint in the list of computers and verify the status. An 🍀 icon indicates that Traps is running on the endpoint. To view additional details about the endpoint, select the endpoint row.
Manage Traps in a VDI Environment

- VDI Overview
- VDI Installation Considerations
- Set Up Traps in a VDI Environment
- Configure the Master Policy
- Configure Traps Settings
- Tune and Test the VDI Policy
VDI Overview

Your rapidly changing business environment demands a flexible infrastructure to support the evolving desktop, application, and data access requirements of your staff. By implementing a virtual desktop infrastructure (VDI), you can empower your employees to work independent of location using a variety of devices.

Although a VDI solution presents many desktop security advantages—including centralized control, reduced complexity, and efficient management of user access and privileges—it is critical to ensure that the entire VDI is secure. Securing this new, centralized environment is increasingly difficult. A single IP address can represent thousands of different users all accessing their applications and data using a variety of devices. Users can also have access to other applications in your data center besides their virtual desktop. By using Traps to secure your VDI environment, you can take advantage of the following benefits:

- Advanced endpoint protection as part of the Traps solution that prevents sophisticated vulnerability exploits and unknown malware-driven attacks.
- A highly scalable, lightweight Traps agent that uses an innovative new approach for defeating attacks without requiring any prior knowledge of the threat.
- Software that is not dependent on scanning or maintaining external updates.

The following topics describe the VDI deployments in more detail:

- Virtualized Applications and Desktops
- VDI Modes

Virtualized Applications and Desktops

- **XenApp**
- **XenDesktop**

**XenApp**

A XenApp is a virtual application that you can manage using a XenApp server. To secure the virtual applications, you must install Traps on the XenApp server that handles the sessions. Instead of using the VDI license on the XenApp server, you must install a single Traps server (most common) or a workstation license based on the operating system of the XenApp server. In this instance, the single Traps installation protects all concurrent sessions.

**XenDesktop**

A XenDesktop delivers virtual applications and desktops to any device. To secure the virtual desktop, install Traps on each virtual desktop instance and install a VDI license from the ESM Console. In addition, we recommend you install the Traps agent on each host operating system. The host operating system requires a separate non-VDI license depending on the operating system of the host: either a server or a workstation license.

> Replacing the host-based antivirus software with Traps can reduce the overall resource consumption.

**VDI Modes**

- **Non-Persistent VDI Mode**
- **Persistent VDI Mode**
Non-Persistent VDI Mode

When a user accesses a non-persistent virtual desktop and logs out at the end of the day, none of their settings or data—including desktop shortcuts, backgrounds, or new applications—are preserved. At the end of a session, the virtual desktop is wiped clean and reverts back to the original pristine state of the master image. The next time the user logs in, they receive a fresh image.

The procedures in this document primarily focus on deploying Traps in a non-persistent VDI mode.

Persistent VDI Mode

A persistent virtual desktop is a one-to-one mapping of a virtual machine to a user and each virtual desktop stores and operates using its own disk image. In this model, a persistent desktop keeps all configuration changes and personalization settings a user makes during a session (such as, background changes, saved shortcuts, and newly installed applications).

When the user ends a session and logs out of the virtual desktop, the virtual machine preserves any and all changes and the next time the user logs on to the desktop, those changes are still in effect.

The process of deploying Traps in persistent VDI mode is very similar to deploying Traps on a standard server or workstation. To install the Traps agent, you can install the Traps software on the master image and run it on the virtual desktop the same as any other VDI application and, just as in a standard deployment, Traps continues to communicate with the ESM Server throughout the life cycle of the VDI instance.
VDI Installation Considerations

- VDI Agent Licenses
- Best Practices for VDI Deployments

VDI Agent Licenses

The ESM Console supports dedicated licenses for virtual desktop infrastructure (VDI) environments and displays the license capacity on the dashboard.

VDI environments can be complex and offer variations based on vendor options and implementation methods. Choose the license that is suitable for your environment:

<table>
<thead>
<tr>
<th>License Type</th>
<th>Description</th>
<th>Revoke Conditions</th>
</tr>
</thead>
</table>
| Workstation/Server License    | Use a standard workstation/server license if your VDI sessions must remain active regardless of the user connectivity (login) status. In this deployment, every VDI session receives a standard workstation/server license that persists after the user logs off thus ensuring that Traps protection is uninterrupted after the user logs off. After the ESM detaches the license, it returns it to the pool of licenses for use by another workstation or server. | The ESM automatically revokes the license only if Traps was uninstalled. To revoke the license on-demand you can:  
• Initiate an action rule (see Update or Revoke the Traps License on the Endpoint)  
• Use the detach method from the ESM Console (see Detach a Traps License) |
| VDI License (PAN-TRAPS-V)     | Use a VDI License for on-demand license distribution. In this deployment, the ESM uses a floating license model to issue the license when a user logs in to a VDI and automatically revoke the license after the session ends. After the ESM detaches the license, it returns it to the VDI pool of licenses for use by another active session. | The ESM automatically revokes the license when any of the following occur:  
• The user logs off.  
• The agent hasn't responded to two consecutive heartbeat communication messages.  
• The agent was uninstalled. To revoke the license on-demand you can:  
• Initiate an action rule (see Update or Revoke the Traps License on the Endpoint)  
• Use the detach method from the ESM Console (see Detach a Traps License) |

The license freeing mechanism operates independently from persistent and non persistent modes.
Best Practices for VDI Deployments

- Optimize the default session policy on the VDI test pool to assure stable session spawning when the VDI is recompiled.
- Every new VDI creation will start with the initial policy as configured on the master image. When the master image is up and communicating with the ESM Server, test the policy on the VDI test pool and push it to the VDI Traps agents. Then fine tune the policy.
- Issues on restricted non-persistent sessions are harder to investigate because there is no forensic data after the session closes. Consider the following options to ensure forensic data is available:
  - Enable the **Send the memory dumps automatically** agent setting on all non-persistent hostnames.
  - Reproduce the issue on a persistent session to collect logs and memory dumps and allow additional troubleshooting.
- Set a fixed number of session hostnames (not random) as licenses are issued by the ESM Console according to hostname. All naming conventions are supported.
- The ESM Server automatically revokes a license when an agent logs off of a VDI session. In cases where the VDI session is not properly closed, the ESM server waits for a timeout before automatically revoking the license to make it available for other VDI agents. If another VDI session needs to use the license before the timeout expires, use the ESM Console to forcefully Detach a Traps License.
Set Up Traps in a VDI Environment

Use the following workflow to set up Traps in a VDI environment.

STEP 1 | Review the installation considerations and prerequisites of the software.
- Endpoint Infrastructure Installation Considerations
- Prerequisites
- VDI Installation Considerations

STEP 2 | Configure the database server.
- Database Software Requirements
- Configure the MS-SQL Server Database

STEP 3 | Set up the ESM Server.
- ESM Server Software Requirements
- Install the Endpoint Security Manager Server Software

STEP 4 | Set up the ESM Console.
- ESM Console Software Requirements
- (Optional) TLS/SSL Encryption for Traps Components
- Install the Endpoint Security Manager Console Software

STEP 5 | Upload the dedicated VDI license.
- VDI Agent Licenses
- Add a Traps License Using the ESM Console

STEP 6 | Install Traps on the master image with the default policy.
- Configure the Master Policy

STEP 7 | Configure additional Traps settings based on your VDI deployment scenario.
- (Recommended) Configure Traps for a Non-Persistent Storage Scenario
  or
  - Configure Traps for a Persistent Storage Scenario

STEP 8 | Configure the initial policy for the master image.
- If your organization supports a mixed environment of VDI and non-VDI instances, apply the Condition for VDI Machine to each rule. This ensures that the rules apply to only the VDI instances.
  - Configure Traps to clear all prevention data and history from the agent. To do this, create an agent action rule (see Manage Data Collected by Traps).
  - Enable Traps to send memory dumps automatically. To do this, create an action rule (see Define Memory Dump Preferences).

STEP 9 | Deploy the VDI test pool.
Tune and Test the VDI Policy

STEP 10 | Recompile the master image.
1. Restart the master image.
2. Verify that the master image can connect to the ESM Server.
3. Shut down the master image and then recompile it.
Configure the Master Policy

To configure the policy for the master image, first collect all portable executable (PE) files using the Windows Sysinternals utility called Sigcheck. Then you can use the Traps VDI tool (either the graphical interface or the command-line interface) to create a WildFire cache file containing the verdicts for all the PE files detected on the master image including any that WildFire determined to be malicious. By replacing the original cache file with the new file, you can avoid many initial unknown verdicts on the VDI instance. You can also use the Traps VDI tool to identify the master image as a VDI instance in the Windows registry.

After identifying the master image as a VDI instance, the ESM Console will recognize the client and use the floating license model to allocate a license.

- Prerequisites for Configuring the Master Policy
- Use the Traps VDI Tool to Configure the Master Policy
- Traps VDI Tool CLI

Prerequisites for Configuring the Master Policy

Use the following workflow to prepare the master image.

STEP 1 | Install any software that you plan to have on the VDI instances.

If after completing the process to configure the master policy, you need to install additional software, you must recreate the WildFire cache file using the Traps VDI tool. This ensures that Traps obtains verdicts for the new software.

1. Install Traps on the master image (see Install Traps on the Endpoint).
2. Install additional required software.

STEP 2 | Verify that the master image can access the ESM Server.

On the Traps agent, click Check-in Now to obtain the latest verdicts from the ESM Server. If the ESM Server is reachable, the status on the console displays Connected.

STEP 3 | Use Cytool to stop the Traps service on the endpoint.

See Start or Stop Traps Runtime Components on the Endpoint.

STEP 4 | Collect all PE files available on the master image using Sigcheck. This tool creates a file for you to use as input for the Traps VDI tool.

2. Open a command prompt as an administrator and navigate to the directory to which you downloaded Sigcheck.
3. Run Sigcheck recursively to find executable files regardless of extension and output the hashes in comma-separated format to a folder and file name of your choice. For example, in Sigcheck version 2.2, use the following command to perform this action:

```
sigcheck /accepteula -s -h -e -q -c C:\ > C:\temp\outfilename.csv
```

The Sigcheck parameters are subject to change. To display available usage guidelines, run the sigcheck command without options.
Use the Traps VDI Tool to Configure the Master Policy

To avoid starting your VDI with a cache of unknown executable files, use the VDI Tool to request verdicts for all known PEs on your master image.

There are two versions of the VDI Tool: 32-bit and 64-bit. Use the version of VDI Tool that matches the VDI architecture.

**STEP 1** | Before you begin...

See Prerequisites for Configuring the Master Policy.

**STEP 2** | Use the Traps VDI Tool to obtain verdicts for all PE files (collected in 4).

A command-line version of the Traps VDI Tool is also available. See Traps VDI Tool CLI.

The Traps VDI tool communicates with the ESM Server to request any verdicts the server has stored in its server cache. The Traps VDI tool then creates a file called WildFireCache.xml which can contain any of the following verdicts for each hash: malicious, benign, or unknown. A hash has an unknown verdict if the ESM Server has not submitted the sample to or received an updated verdict from WildFire.

1. Open the Traps VDI tool.
2. Configure the following settings:
   - **ESM server address**—IP address or hostname of the ESM Server used for checking the hashes. This server must be able to connect to WildFire.
   - **ESM server SSL binding**—Set the value to True if the server uses an SSL binding (default is False).
   - **Input file**—Path of the comma-separated value (CSV) file that you created in 4 that contains all the hashes.
   - **Output file path**—Enter the filename that the Traps VDI tool will use to create the WildFire cache output: WildFireCache.xml. The Traps VDI tool creates the file in the same folder as the tool unless you changed the path here.
- **ESM server port**—Port number for the ESM server (default is 2125).
- **Hash bulk size**—Hashes will be reported to the server in fragments of this size (default is 300; range is 1 to 500).
- **Tool timeout in hours**—Time in hours to wait for the Traps VDI tool to finish obtaining verdicts. If the Traps VDI tool exceeds the timeout, it stops generating the WildFire cache (default is 24 hours).
- **Wait for WildFire verdicts**—Select False to skip uploading unknown hashes and creating the cache file.
- **WildFire verdicts check interval**—Time in minutes between inquiries to check for new verdicts (default is 10).
- **Write malware to cache**—Select True to write malware verdicts to the cache file (default is False).

3. Click **Start**.

The Traps VDI tool uses the results of the verdict lookup to create the WildFireCache.xml file.

4. Wait two hours for the ESM Server to query WildFire for any unknown verdicts and then proceed to the next step. During this time, the ESM Server populates the server cache with any verdicts for hashes WildFire has previously analyzed.

**STEP 3 |** Submit any remaining unknown executable files for analysis. The Traps VDI tool uploads the files to the ESM Server which then sends the files to WildFire for inspection. After the ESM Server submits the samples, the server queries WildFire every 10 minutes for updated verdicts.

1. Open the Traps VDI tool.
2. Change the **Wait for WildFire verdicts** setting to **True**. This setting enables the Traps VDI tool to send any remaining unknown executable files and wait for the WildFire verdict.
3. Click **Start**.

After the verdict lookup is complete, the Traps VDI tool recreates the XML file containing the hashes and their verdicts.

**STEP 4 |** Review any PE files that WildFire determined to be malicious.

1. Open the Malware text file created by the Traps VDI tool. This file contains the list of hashes for which WildFire returned a malicious verdict.
2. Perform one of the following actions for each malicious PE file:
   - Remove the malicious PE file from the master image.
   - If you believe the WildFire verdict is incorrect, override the verdict for the PE file on the Hash Control page of the ESM Console and change the verdict to benign in the WildFireCache.xml.

**STEP 5 |** Terminate the agent service and drivers using Cytool.

See Start or Stop Traps Runtime Components on the Endpoint.

**STEP 6 |** Replace the WildFire cache with the file generated by the Traps VDI tool.

1. Locate the WildFire cache file generated by the Traps VDI tool. The file is located in the path that you specified in the **Output file path** field.
2. Replace WildFireCache.xml file with the new file in %ProgramData%\Cyvera\LocalSystem\.

**STEP 7 |** Use the Traps VDI tool to identify the master image as a VDI instance.

1. Open the Traps VDI tool.
2. Click the **Menu** in the top left corner and select **Mark as VDI**.
3. Enter the Traps uninstall password and click **Mark as VDI**.

The tool identifies the machine in the Windows registry as a VDI instance.
STEP 8 | Ensure the ESM Server can access WildFire.

From the ESM Server, open a browser to the following address: https://wildfire.paloaltonetworks.com.

**Traps VDI Tool CLI**

The Traps VDI Tool requests verdicts for all the PE files detected on the master image and outputs the verdicts to a WildFire cache file. You can use the command-line interface (CLI) version of the Traps VDI Tool to automate the creation of this file.

Consider the following usage guidelines for the Traps VDI Tool CLI:

- If you run the Traps VDI Tool with at least one command line argument, it will run in unattended mode (no user interface). If you issue the `TrapsVdiTool` command without any arguments, the user interface opens.
- By default, arguments with flag values—yes or no—default to yes. Therefore, to use the default value, you can specify the argument without the value (e.g. use `-ssl` instead of `-ssl:y`).
- If a path value contains one or more spaces, surround the entire path argument with double quotes, for example: `"-i:c:\temp\sig file.csv"`.
- You cannot use the Traps VDI Tool to check hashes and mark the computer as a VDI—using the `-m` argument—at the same time. Therefore, you must execute these actions separately.
- To write output to a log file, use the `>` redirect to send output to a filename of your choice, for example: `TrapsVdiTool -m > TrapsVDI.log`

**STEP 1 |** Download and unzip the Traps VDI Tool on the master image.

**STEP 2 |** Open a command prompt as an administrator:

- Select **Start** > **All Programs** > **Accessories**. Right-click **Command prompt**, and then select **Run as administrator**.
- Select **Start**. In the **Start Search** box, type **cmd**. Then, to open the command prompt as an administrator, press **CTRL+SHIFT+ENTER**.

**STEP 3 |** Navigate to the folder that contains the Traps VDI Tool CLI:

```
c:\Users\Administrator>cd C:\TrapsVDItool
```

**STEP 4 |** View usage and options for the DB Configuration Tool:

```
c:\TrapsVDItool> TrapsVdiTool -help
[...]
Usage:
TrapsVdiTool -help
TrapsVdiTool -m:password
- help Displays the help screen.
- silent Perform tasks in silent mode (no log displays).
- i:path Input file (must be CSV). Specifies the path of the file produced by the sigcheck tool. No default. Surround the entire path argument with double quotes to specify a path that contains spaces, for example: "-i:c:\temp\sig file.csv".
- o:path Output file path. Specifies the full XML path. Default:
```
current directory. Surround the entire path argument with double quotes to specify a path that contains spaces, for example: "-o:C:\temp folder \WildFireCache.xml".
-e:address Specifies the ESM server address (FQDN or IP). Default: ESMSERVER
-p:port Specifies the ESM server port. Default: 2125
-ssl[:flag] ESM server SSL binding. Indicates use of secured server connection. 'y' for using SSL, 'n' otherwise. Default: n
-b:size Hash bulk size. Specifies the bulk size for hash transfers. Default: 300
-to:hours Tool timeout in hours. Limits execution time to specified number of hours. Default: 24
-c:minutes Specifies WildFire verdicts check interval in minutes. Default: 10
-r[:flag] Instructs the tool to continue from where it left off previously. Default: n
-w[:flag] Write malware verdicts to cache. Default: n
-g[:flag] Write grayware verdicts to cache. Default: y
-m:password Instructs the Traps VDI Tool to identify this computer as VDI using the uninstall password and skips performing hash checks. No default. Do not use this option if you want the Traps VDI Tool to perform hash checks.

STEP 5 | Specify arguments to create the WildFire cache file or to mark the master image as a VDI instance. For example:

• **TrapsVdiTool -i:c:\temp\sig.csv -e:192.168.70.100 -ssl -to:1**

The Traps VDI Tool requests verdicts for the hashes in the c:\temp\sig.csv input file, from the ESM Server with the IP address 192.168.70.100, over a secure connection, and limits the execution time to 1 hour.

All the other arguments are set to their default values.

• **TrapsVdiTool "-i:c:\temp\sig file.csv" -v -w**

The Traps VDI Tool requests verdicts for the hashes in the c:\temp\sig file.csv input file from the default ESM Server, and creates the cache file only after it has received verdicts for all hashes. Note the file path is enclosed in quotes because the filename contains a space.

• **TrapsVdiTool -m:password**

The Traps VDI Tool identifies the master image as a VDI instance without performing hash checks.
Configure Traps Settings

Before configuring additional Traps settings, you must Configure the Master Policy. Then configure settings according to your type of VDI deployment:

- Configure Traps for a Non-Persistent Storage Scenario
- Configure Traps for a Persistent Storage Scenario

Configure Traps for a Non-Persistent Storage Scenario

In a non-persistent storage scenario, the Traps services use an automatic delayed start. Additionally, you must configure the services to restart after a failure to ensure that the Traps agent sends a heartbeat to the ESM Server soon after the service starts to obtain the latest policy.

**STEP 1 | Configure Traps services on the master image.**

1. Open services.msc: Click Start > Run, enter services.msc, and then press Enter.
2. Right-click the Traps service and select Properties.
3. From the service Startup type drop-down, select Automatic (Delayed Start).
4. Click Apply and then OK.
5. Repeat the process for the Traps Dump Analyzer Service and Traps Reporting Service.

**STEP 2 | Configure the Traps service with a dependency on the Spooler Service (or any of the other last loading services) per the following Microsoft KB [http://support.microsoft.com/kb/193888](http://support.microsoft.com/kb/193888).**

1. Open the Windows Registry and locate the CyveraService key in HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\
2. Double-click the DependOnService multistring.
3. Add Spooler to the Value data list.
4. Click OK.

Configure Traps for a Persistent Storage Scenario

If utilizing a VDI machine to offload to a local storage area, you need to make additional changes to the master image, including changes to the Traps service properties and the startup and shutdown scripts.

STEP 1 | Create a symbolic link from the machine's standard drive to the machine's local storage each time the VDI boots.

On the master image, run the **Startup Script** using GPO or schedule it to run as a task or local policy.

To configure GPO for startup scripts:

1. Run gpmc.msc (Group Policy Management) on your domain controller and then create a new GPO.
2. Give the GPO a meaningful name and click **OK**.
3. Right-click on the newly created GPO and select **Edit**.
4. In the left pane of the Group Policy Management Editor, navigate to **Scripts (Startup/Shutdown)**, and then go to the right pane and double-click **Startup**.
5. Click **Add**, navigate to your script, select your script, and click **OK**.

STEP 2 | Reset the services state before the image is sealed and migrated into a test or production environment.

On the master image, create a batch file using the **Shutdown Script** and then run it.

STEP 3 | Configure Traps services.

1. Open services.msc: Click **Start > Run**, enter services.msc, and then press Enter.
2. Right-click the **Traps** service and select **Properties**.
3. From the service **Startup type** drop-down, select **Manual**.
4. Click **Apply** and **OK**.
5. Repeat the process for the **Traps Dump Analyzer Service** and **Traps Reporting Service**.

**Startup Script**

```
set drivepath=D:\
set datapath=%drivepath%\ProgramData\Cyveraset
set policypath=%ProgramData%\CyveraNotInUse\LocalSystem\ClientPolicy.xml
IF EXIST %drivepath% ( 
IF EXIST %ProgramData%\Cyvera ( 
rename %ProgramData%\Cyvera Cyvera CyveraNotInUse
```
%windir%\system32\cmd.exe /c mklink /J %ProgramData%\Cyvera %datapath% 2>&1
IF NOT EXIST %datapath% ( mkdir %datapath% )
IF NOT EXIST %datapath%\Everyone\Data ( mkdir %datapath%\Everyone\Data )
IF NOT EXIST %datapath%\Everyone\Temp ( mkdir %datapath%\Everyone\Temp )
IF NOT EXIST %datapath%\LocalSystem ( mkdir %datapath%\LocalSystem )
IF EXIST %datapath%\LocalSystem\ClientPolicy.xml ( del /F %datapath%\LocalSystem\ClientPolicy.xml )
copy %policypath% %datapath%\LocalSystem\ClientPolicy.xml
IF NOT EXIST %datapath%\LocalSystem\Data ( mkdir %datapath%\LocalSystem\Data )
IF NOT EXIST %datapath%\Logs ( mkdir %datapath%\Logs )
IF NOT EXIST %datapath%\Prevention ( mkdir %datapath%\Prevention )
)
sc start cyserver
sc start cyveraservice
sc start TrapsDumpAnalyzer
time /t >> %datapath%\Logs\gpolog.txt

Shutdown Script

::Stop Cyvera services
net stop CyveraService
net stop TrapsDumpAnalyzer
net stop CyServer
rd c:\ProgramData\Cyvera /q
ren c:\ProgramData\CyveraNotInUse Cyvera

net start CyveraService
net start TrapsDumpAnalyzer
net start CyServer
Tune and Test the VDI Policy

After you configure the master policy, tune and test the policy using the following workflow.

**STEP 1 |** Install Traps on a test machine (either the master image or a non-VDI instance) and fine-tune the exploit and malware protection policies.

Use the built-in VDI condition to apply rules to VDI instances only.

**STEP 2 |** Use the master image to spawn a small pool of persistent sessions (2 or 3). Deploy the sessions in a production environment and imitate the expected day-to-day user behavior, such as browsing, development, and dedicated application usage.

**STEP 3 |** Gather additional information during this period to further optimize the default session policy and test any special restrictions applied to the non-persistent sessions. Typically, clients deployed in persistent mode enable better forensics collection than clients deployed in non-persistent mode.

**STEP 4 |** Resolve any stability issues on the test machine and on the test VDI pool that were caused by the exploit or malware protection policies.

**STEP 5 |** After the VDI server spawns a session from the master image and connects to the ESM Server, disconnect the master image. Then revise the VDI policy so that WildFire integration is enabled, EPM Injection is set according to the configuration tested on the master image, heartbeat and reporting settings use longer intervals (60 minutes is recommended), and memory dumps are sent automatically.

Traps will replace the initial master policy with the revised VDI policy. Changing the VDI policy affects all spawned session on the next restart.

**STEP 6 |** Log into the ESM Console and verify the health of the VDI instances on the **Monitor > Agent > Health** page. If your organization uses a mixed environment, you can filter the machine Type column to show only VDI instances. The status of the VDI instances should be connected.
Administer the ESM Server

- Manage ESM Server Settings
- Manage ESM Console Settings
- Manage Multiple ESM Servers
- Traps Licenses
- Manage Administrator Access to the ESM Console
- Export and Import Policy Files
Manage ESM Server Settings

The ESM Server facilitates communication between Traps agents and WildFire.

The ESM Server periodically communicates with WildFire to:

- Send unknown files for analysis
- Request verdicts associated with executable files
- Submit requests to reanalyze a file

The ESM communicates with Traps agents to perform three primary tasks:

- Retrieve the operational status of the agent
- Obtain reports on processes running on the endpoint
- Send the latest security policy.

You can change the frequency of these communications between the server and the endpoint using the Database (DB) Configuration Tool (see Configure ESM Server Settings Using the DB Configuration Tool) or using the ESM Console.

STEP 1 | From the ESM Console, select Settings > ESM > Settings.

STEP 2 | Configure any of the following settings for the ESM Server:

- **Quarantine Network Path**—(Traps 3.1 and earlier versions) Default forensic folder to use when the Traps agent cannot reach the folder associated with the ESM Server to which the agent is connected.
- **Inventory Interval (Minutes)**—Enter the frequency at which Traps sends a list to the ESM Server to report the applications that are running on the endpoint.
- **Heartbeat Grace Period (Seconds)**—Enter the allowable grace period for a Traps agent that has not responded (range is 300 to 86,400; default is 4200).
- **Forensic Folder URL**—BITS-enabled forensic folder URL.

  To encrypt forensic data, we strongly recommend that you use SSL to communicate with the forensic folder. To use SSL, include the fully qualified domain name (FQDN) and specify port 443 (for example, HTTPS://ESMserver.Domain.local:443/ BitsUploads). If you do not want to use SSL, specify port 80 (for example, http://ESMSEVER:80/BitsUploads).

- **Keep-alive Timeout**—Timespan (in minutes) where the endpoint sends a keep alive message to the log or report (range is 0 or greater; default is 0).
- **Update From Server Package Address**—Externally accessible URL of the ESM Console used to host upgrade packages for Traps agents. By default, when you configure an action rule to upgrade the Traps software, the rule is configured to use the ESM Console hostname. If the ESM Console is accessible by the DNS record only and not by the default ESM Console hostname, use this field to specify a URL beginning with an HTTP or HTTPS prefix followed by the DNS record.

  If you do not specify a server URL in this field, the action rule to upgrade agents uses your current session to determine the SSL preference. For example, if you log into the ESM Console using HTTP and create an action rule to upgrade the agents, the agents receive an upgrade path with an HTTP prefix. If you log in using HTTPS, the agents receive an HTTPS prefix.

- **Use DNS For Address Resolution**—Select this option to enable DNS for address resolution. By default, this option is disabled to prevent excessive DNS error logging.
STEP 3 | (Optional) For deployments that use multiple ESM Servers, you can also configure each ESM Server to communicate with WildFire through a proxy server.

1. Select **Settings > ESM > Multi ESM**.
2. Select the row for the ESM Server for which you want to configure proxy communication. The ESM Console displays the settings associated with the server.
3. Select **Edit**.
4. Enable **Proxy** communication.
5. Enter the FQDN or IP address of the proxy server in the **Proxy Host/IP** field and a **Proxy Port** number (default is 8080). Optionally, enable **Proxy Authentication** and then enter the **Username** and **Password**—using only ISO-8859-1 characters—the ESM Server will use to authenticate with the proxy server.
6. **Save** your changes to the ESM Server settings.
7. Repeat this process to configure proxy configuration for other ESM Servers, if desired. You can configure the same proxy settings across multiple ESM Servers, or configure proxy settings that are unique to each server.

For more information, see **Manage Multiple ESM Servers**.

STEP 4 | **Save** your changes.
Manage ESM Console Settings

From the ESM Console, you can configure the following settings for the server that hosts the console:

- Dashboard display period
- User authentication mode used to authenticate users who log in to the ESM Console, either machine or domain
- Proxy server to facilitate communication between the ESM Console and WildFire.

**STEP 1** | From the ESM Console, select **Settings > ESM > Settings**.

**STEP 2** | Configure any of the following settings for the ESM Console:

- **Dashboard Display Period (Days)**—Number of days used to generate dashboard charts and graphs. By default, the ESM Console displays information collected over the past 30 days (range 1-10,000).
- **User Authentication Mode**—Method to authentication ESM Console users, either **Machine** (local), or **Domain**.
- **Proxy**—Enter the FQDN or IP address of the proxy server in the **Proxy Host/IP** field and a **Proxy Port** number (default is 8080). Optionally, enable **Proxy Authentication** and then enter the **Username** and **Password**—using only ISO-8859-1 characters—the ESM Console will use to authenticate with the proxy server.

**STEP 3** | **Save** your changes.
Manage Multiple ESM Servers

To support large scale or multi-site deployments, you can configure and manage multiple Endpoint Security Manager (ESM) Servers from the ESM Console. Each ESM Server connects to a shared database that stores security policies and information about Traps agents and events and can upload forensic data to a dedicated forensic folder. Adding additional ESM Servers allows you to scale the number of Traps connections that can connect to your network.

- Known Limitations with Multi-ESM Deployments
- What Logic Does the Agent Use When Selecting an ESM Server?
- Activate, Disable, or Delete an ESM Server

Known Limitations with Multi-ESM Deployments

In a multi-ESM deployment, each ESM Server must meet the requirements specified in ESM Server Software Requirements. Multi-ESM deployments also have the following limitations:

- **Load balancing**—To use a load balancer to manage traffic between multiple ESM Servers, you must specify the IP address of the load balancer—instead of the ESM Server—when you install the Traps agent. The Traps agents can then establish connections through the load balancer instead of attempting to connect directly to an ESM Server.
- **IP addressing**—Each ESM Server must have a static IP address.
- **Scaling**—You can install a maximum of five ESM Servers. To install additional servers, contact your Sales Engineer.

What Logic Does the Agent Use When Selecting an ESM Server?

At regular heartbeat intervals, the Traps agent receives a list of all known ESM Servers. To evaluate the ESM Server to which the agent will connect, Traps considers the priority and TTL (in terms of number of hops) for each server. Traps prioritizes the list of ESM Servers by internal IP address (priority 1), external IP address (priority 2), followed by the ESM Server specified during the agent installation (priority 3). For example, consider the following scenario with four ESM Servers:

<table>
<thead>
<tr>
<th>ESM Server</th>
<th>Internal Address TTL</th>
<th>External Address TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>C</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>D (default install)</td>
<td>2</td>
<td>5</td>
</tr>
</tbody>
</table>

After evaluating the TTL value for each ESM Server, Traps builds an ordered list:

Priority=1, TTL=1, Latency=10.00ms, Address=https://esmsserverB.example.com:2125/
Priority=1, TTL=2, Latency=20.00ms, Address=https://esmsserverA.example.com:2125/
Priority=1, TTL=2, Latency=20.00ms, Address=https://esmsserverC.example.com:2125/
Priority=2, TTL=3, Latency=30.00ms, Address=https://10.31.32.1:2125/
Priority=2, TTL=4, Latency=40.00ms, Address=https://10.31.32.2:2125/
Priority=2, TTL=5, Latency=50.00ms, Address=https://10.31.32.3:2125/
Priority=3, TTL=2, Latency=20.00ms, Address=https://esmserverD.example.com:2125/

In this example, ESM Server B has the lowest TTL value (fewest number of hops) and highest priority. If Traps cannot establish a connection to ESM Server B—the preferred ESM Server—it moves on down the list until it is able to successfully establish an ESM Server connection.

In the event of a tie—where two ESM Servers have the same priority and the same TTL value—the Traps agent selects a server at random.

If no ESM Servers are reachable (the ESM Server list is empty), the agent status changes to No Connection. After a period of inactivity, the agent tries to connect again (by default once every minute or as specified in an Agent Settings communication rule). The Traps agent also periodically verifies the integrity of the ESM Server list (by default once every hour or as specified in an Agent Settings communication rule). The Traps agent can also immediately validate the list of ESM Servers when any of the following occur:

- The network address of the endpoint changes
- The endpoint resumes or restarts
- The IP address for an ESM Server changes
- A manual Check-In Now is initiated from the Traps console
- A communication request from the agent to the server times out or fails

If you remove or temporarily disable an ESM Server, the ESM Console removes the ESM Server from the list of available ESM Servers and pushes it to Traps agents at the next heartbeat. However, if you specified the (now disabled) ESM Server during the Traps installation, those agents retain the (priority 3) ESM Server in the list of available ESM Servers to which they can connect.

Activate, Disable, or Delete an ESM Server

After installing each ESM Server (see Install the Endpoint Security Manager Server Software), the ESM Console displays identifying information about each server on the Settings > ESM > Multi ESM page.

You can modify the configuration settings for the ESM Servers at any time. You can also temporarily disable, activate, or remove an ESM Server, as needed.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ESM Server Settings</td>
<td>See Manage ESM Server Settings.</td>
</tr>
<tr>
<td>Disable an ESM Server</td>
<td>Select <strong>Disable Selected</strong> from the action □ menu at the top of the page. The ESM Console changes the status of the server to <strong>Disabled</strong>. This action temporarily removes the ESM Server from the available server</td>
</tr>
<tr>
<td>Action</td>
<td>Steps</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Delete an ESM Server</td>
<td>Select Delete Selected from the action menu at the top of the page. This action permanently removes the ESM Server from the ESM Console and from the available server pool of ESM Servers to which the Traps agents can connect; However, if the ESM Server was specified during the Traps installation, the agent retains the ESM Server on its list of available servers. You cannot reactivate a deleted ESM Server unless you first reinstall it.</td>
</tr>
<tr>
<td>Activate an ESM Server</td>
<td>Select Activate Selected from the action menu at the top of the page. This action adds the disabled ESM Server back in to the available servers pool.</td>
</tr>
</tbody>
</table>
Traps Licenses

- About Traps Licenses
- Add a Traps License Using the ESM Console
- Add a Traps License Using the DB Configuration Tool
- Detach a Traps License

About Traps Licenses

A Traps license enforces the expiration date and maximum number of endpoints that you can manage from the ESM Console. Endpoints retrieve their licenses from the ESM Server and each license specifies the license type (server, workstation, or VDI), agent pool size, and expiration date.

To determine which license to use for a VDI environment, see VDI Agent Licenses.

Each database instance requires a valid license that entitles you to manage the endpoint security policy, enable WildFire, and obtain support. To purchase licenses, contact your Palo Alto Networks Account Manager or reseller.

You can manage licenses in the following ways:

- **View license utilization**—Use the License Capacity chart on the Dashboard to view the current utilization of all client, server, and VDI licenses.
- **Add a Traps license**—Use the Settings > License page to add support for additional features or users. See Add a Traps License Using the ESM Console.
- **Update a license**—To update the license for an endpoint, create an action rule specifying the target endpoints that require a license update. See Update or Revoke the Traps License on the Endpoint.
- **Revoke a license**—To temporarily revoke a license from an endpoint, you can Detach a Traps License from an endpoint on the ESM Console. This action immediately updates the available pool of licenses and frees up the license for use by another Traps agent. The Traps agent remains unlicensed until the Traps service or endpoint reboots. At this time, the agent attempts to establish communication with the ESM Server and requests a new license. To permanently revoke a license from an endpoint, you can create an action rule for the target endpoint (see Update or Revoke the Traps License on the Endpoint). When Traps receives the action rule at the next heartbeat communication with the ESM Server, Traps releases the license and turns off Traps protection.

Add a Traps License Using the ESM Console

Before you can start using Traps to protect your endpoints, you must install a valid license key.

**STEP 1** | Before you begin: Obtain a license from your Palo Alto Networks Account Manager or reseller.

**STEP 2** | Select Settings > Licensing and then Add a new license.

**STEP 3** | Browse to and then Upload the license file. The ESM Console displays information about the new license, including the license features, the agent pool size, the number of endpoints to which the license has been issued, the date you added the license, and the date the license expires.
STEP 4 | (Optional) To verify the Traps license utilization, select Dashboard and view the License Capacity.

STEP 5 | (Optional) To push the new license to endpoints that are nearing or have exceeded the license expiration date, create an action rule (see Update or Revoke the Traps License on the Endpoint).

STEP 6 | (Optional) To export the license information to a CSV file, click the action menu ≈ , and then select Export Logs.

STEP 7 | If you did not install the license key during the installation of the ESM Console, verify that the Endpoint Security Manager core service is running on the ESM Server:

1. Open the Services Manager either by navigating to it from the Control Panel or by searching for Services Manager from Start > Run.
2. Locate the Endpoint Security Manager service and verify that the service status is Started (Windows Server 2008) or Running (Windows Server 2012).
3. If the service status is Stopped or Paused, double-click the service, then select Start.
4. Click Close.

Add a Traps License Using the DB Configuration Tool

Using the Database (DB) Configuration Tool, you can manage basic ESM Server settings, including the ability to install a license. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt that you run as an administrator. The DB Configuration Tool is located in the Server folder on the ESM Server.

All commands you run using the DB Configuration Tool are case sensitive.

STEP 1 | Before you begin: Obtain a license from your Palo Alto Networks Account Manager or reseller.

STEP 2 | Open a command prompt as an administrator in either of two ways:

- Select Start > All Programs > Accessories, right-click Command prompt, and then select Run as administrator.
- Select Start and in the Start Search box, type cmd but do not press Enter, yet. Then, to open the command prompt as an administrator, press Ctrl+Shift+Enter.

STEP 3 | Navigate to the folder that contains the DB Configuration Tool:

C:\Users\Administrator>cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server

STEP 4 | Upload the new license:

C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig importLicense C:\<PathToLicenseFile>\<LicenseFilename>.xml

The DB Configuration Tool uploads the license file. To verify the license using the ESM Console, see Add a Traps License Using the ESM Console.
STEP 5 | *(Optional)* If necessary, create an action rule in the ESM Console to push the new license to the endpoints (see Update or Revoke the Traps License on the Endpoint).

**Detach a Traps License**

Detaching a license from an endpoint is a temporary action that immediately updates the available pool of licenses and frees up the license for use by another Traps agent. When you detach a license, the Traps agent remains unlicensed until the Traps service or endpoint reboots. When the endpoint reboots, the agent attempts to establish communication with the ESM Server and requests a new license. Detaching a license can be useful in VDI environments where a VDI session did not close correctly and did not release the floating license.

To permanently revoke a license from an endpoint, create an action rule for the target endpoints (see Update or Revoke the Traps License on the Endpoint). This action will release the license and turn off Traps protection during the next heartbeat communication with the Traps agent.

**STEP 1 | Select Monitor > Agent > Health.**

**STEP 2 | Locate the endpoint from which you want to revoke the license.**

*To quickly locate an endpoint such as a computer, use the filter controls at the top of the Computer column.*

**STEP 3 | In the agent health table, select the checkbox for one or more endpoints.**

**STEP 4 | Click the action menu ➔, and then select Detach License. The ESM Server immediately returns the license to the available pool and frees it up for use by another Traps agent.*
Manage Administrator Access to the ESM Console

When you install the Endpoint Security Manager (ESM) Console, you specify the administrative account and type of authentication the administrator will use to access the console. The ESM Console can authenticate users defined on the local ESM Console server or by using domain accounts (including groups and organizational units) defined in Active Directory (AD). After installation, you can change the authentication mode, customize roles with access privileges, and assign those roles to administrative accounts.

- Administrative Roles
- Administrative Users
- Administrative Authentication
- Configure Administrative Accounts and Authentication

Role-based access control (RBAC) enables you to use preconfigured or define custom roles to assign access rights to administrative users. Each role extends specific privileges to users you assign to the role and each privilege defines access to specific configuration settings and pages within the ESM Console. By customizing a role and assigning specific privileges, you can enforce the separation of information among functional or regional areas of your organization to protect the privacy of data on the ESM Console.

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Description</th>
<th>Users in Role</th>
<th>Date Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Full read-write access to the ESM Console.</td>
<td>2</td>
<td>9/11/2015, 2:33:15 PM</td>
</tr>
<tr>
<td>IT Administrator</td>
<td>Read-write access to monitor and configuration settings pages and read-only access to all other pages in the ESM Console.</td>
<td>0</td>
<td>9/9/2015, 2:33:15 PM</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>Read-write access to policy configuration, monitoring, and settings pages in the ESM Console, including the ability to disable all protection.</td>
<td>0</td>
<td>9/9/2015, 2:33:15 PM</td>
</tr>
</tbody>
</table>

The way you configure administrative access depends on the security requirements of your organization. Use roles to assign specific access privileges to administrative user accounts. By default, the ESM Console has built-in roles with specific access rights that cannot be changed. When new features are added to the product, the ESM Console automatically adds new features to the default role definitions. The following table lists the access privileges associated with built-in roles that provide access to the ESM Console:

<table>
<thead>
<tr>
<th>Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Superuser</td>
<td>Full read-write access to the ESM Console.</td>
</tr>
<tr>
<td>IT Administrator</td>
<td>Read-write access to monitor and configuration settings pages and read-only access to all other pages in the ESM Console; does not include the ability to disable all protection.</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>Read-write access to policy configuration, monitoring, and settings pages in the ESM Console, including the ability to disable all protection. This role also includes read-only access to the agent health pages but no access to the server health or licenses pages.</td>
</tr>
</tbody>
</table>

While you cannot change the privileges associated with the built-in roles, you can create custom roles that provide more granular access control over the functional areas of the web interface. For these roles, you
can assign read-write access, read-only access, or no access to all the ESM Console configuration functions and pages.

An example use of a custom role is security administrators who need to be able to view logs about the status of endpoints but who do not need to configure security rules.

Administrative Users

An administrative user is a local or domain user account that has access to specific administrative or reporting functions on the ESM Console. Using role-based access control (RBAC), you can assign specific privileges and responsibilities to a role and then assign that role to one or more users who require the same access permissions.

As a best practice, create a separate administrative account for each person who needs access to the ESM Console. This provides better protection against unauthorized configuration (or modification) and enables logging of all actions for each individual administrator.

Use the ESM Console to assign administrative access to any of the following account types:

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User</strong></td>
<td><em>(Machine or domain authentication)</em> Existing domain or local user account used to log into the ESM Console. The ESM Console authenticates the user in one of two ways:</td>
</tr>
<tr>
<td></td>
<td>• Domain authentication—authenticates using the credentials stored in Active Directory.</td>
</tr>
<tr>
<td></td>
<td>• Machine authentication—authenticates using the credentials stored on the local system on which the ESM Console is installed.</td>
</tr>
<tr>
<td><strong>Group</strong></td>
<td><em>(Domain authentication only)</em> Extends administrative access to all members of a security group and uses the authentication credentials defined in Active Directory to authenticates the user.</td>
</tr>
<tr>
<td><strong>Organizational Unit</strong></td>
<td><em>(Domain authentication only)</em> Extends administrative access to all members of an organizational unit and uses the authentication credentials defined in Active Directory to authenticates the user.</td>
</tr>
</tbody>
</table>

The ESM Console does not retain credentials for any administrative account. To change the credentials of an administrative account, you must modify them on the local machine if using machine authentication or in Active Directory if using domain authentication.
Administrative Authentication

When you install the ESM Console, you specify the administrative user and type of authentication that the ESM Console uses to authenticate administrative users. You can change these preferences using the Database (DB) Configuration Tool (see Configure Administrative Access to the ESM Console Using the DB Configuration Tool) or using the ESM Console (see Configure the Authentication Mode). You can also specify a preexisting authentication group to use for administrative access. By default, no groups are specified.

You can configure the following types of administrator authentication:

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Uses accounts defined in Active Directory—including users, groups, or organizational units—for administrative access.</td>
</tr>
<tr>
<td>Machine</td>
<td>Uses accounts that are local to the ESM Console server for administrative access.</td>
</tr>
</tbody>
</table>

Configure Administrative Accounts and Authentication

- Configure Administrative Roles
- Configure Administrative Users, Groups, or Organizational Units
- Configure the Authentication Mode
- Change the Ninja-Mode Password

Configure Administrative Roles

From the Administration > Roles page, you can see all the built-in and custom roles for your organization. Creating custom roles enables you to tailor the access permissions around the security requirements for your organization.

Each role shows the role name and description, the number of users that are assigned to the role, and the date the role was created. Selecting the row for a role expands that row to display additional details and actions. The actions you can perform on the role vary for both built-in and custom roles.
While you cannot modify or delete any of the built-in roles, you can view the access privileges that are associated with the role. You can, however, add, modify, or delete a custom role. You can also block any role to prevent users that are assigned to that role from logging in to the ESM Console. Similarly, deleting a custom role removes the access privileges associated with that role from the ESM Console and prevents users from logging in to the ESM Console if they are assigned to that role. The ESM Console displays blocked roles with a red icon in the status column.

**STEP 1** | From the ESM Console, select Settings > Administration > Roles. The ESM Console displays all built-in and customized roles for your organization.

**STEP 2** | Select and then Edit an existing role, or Add a new one.

**STEP 3** | Define the Role Name and enter a Description.

**STEP 4** | Select the Is Active option to enable the role or deselect the option to disable the role.

**STEP 5** | Select a privilege to toggle through the different levels of access for that privilege. By default, all privileges are disabled. Selecting the privilege once changes the setting to Read Only access; selecting the privilege again changes the access level to read-write access (Enable); and selecting the privilege from an enabled state disables the privilege.

**STEP 6** | Click Save. The ESM Console displays the new or modified role in the table.

**STEP 7** | Assign the role to a user. See Configure Administrative Users, Groups, or Organizational Units.

Configure Administrative Users, Groups, or Organizational Units

From the Settings > Administration > Users page, you can view all the accounts that provide administrative access to the ESM Console. An account can be a user, a group, or an organizational unit. To provide administrative access to a group or organizational unit, the account must exist on the domain. To provide administrative access to a user, you can add either a user on the local machine or a user on the domain. The ESM Console uses the domain or the credentials defined on the local machine to authenticate the user.

As a best practice, create a separate account for each user that requires access to the ESM Console.

For each account, the ESM Console displays the account status (Blocked or Unblocked), the account Name, the assigned Role, and the date that the account was created. Selecting the row for an account will expand the row to display additional details and actions, including who created the role (System, DbConfig, or the administrative account that is logged into the ESM Console). The actions you can perform on a role vary depending on where the role was created. If you have permissions to do so, you can edit, block, unblock, or delete any account created by other administrative users but you cannot block or delete accounts that were created from DBconfig.
Blocking an account prevents that account from logging in to the ESM Console. Similarly, deleting an account removes the account and settings from the ESM Console and prevents the account from logging in to the ESM Console. When a role that is associated with an account is blocked, the ESM Console displays the Role as <role name> (inactive). When a role that is associated with an account is deleted, the ESM Console displays the Role as N/A (inactive). The ESM Console also displays blocked accounts with a red ⌫ icon in the status column and indicates a deleted or blocked role with a red ⌫ icon next to the Role name.

**STEP 1** | From the ESM Console, select **Settings > Administration > Users**. The ESM Console displays the accounts for your organization, including users, groups, and organizational units.

*If you cannot log into the ESM Console, use the Database (DB) Configuration Tool to verify, and optionally change, the users and groups that have access to the ESM Console (see Configure Administrative Access to the ESM Console Using the DB Configuration Tool).*

**STEP 2** | Click **Add User**, **Add Group**, or **Add Organizational Unit** to create a new account. Alternatively, select the row of an existing account and click **Edit** to modify the account settings. From this view, you can also **Block**, **Unblock**, or **Delete** an account.

**STEP 3** | Enter the **Name** of an existing account. If you are using machine authentication, you can only add existing users on the local machine. If you are using domain authentication, you can add any existing domain user, group, or organizational unit.

*The ESM Console truncates usernames over 20 characters. As a result, users must log in to the ESM Console using only the first 20 characters of their username.*

**STEP 4** | Select the **Is Active** option to enable the account or clear the **Is Active** option to disable the account.

**STEP 5** | Select the role from the list to assign access privileges to the account. To create a new role, see Configure Administrative Roles.

**STEP 6** | **Save** your changes. The ESM Console displays the new or modified account in the table.

**Configure the Authentication Mode**

When you install the ESM Console, you specify the administrative account and type of authentication that administrators will use to access the console. You can change these preferences using the ESM Console as follows:

**STEP 1** | From the ESM Console, select **Settings > ESM > Settings**.

*If you cannot log into the ESM Console, use the Database (DB) Configuration Tool to verify, and optionally change, the authentication mode (see Configure Administrative Access to the ESM Console Using the DB Configuration Tool).*

**STEP 2** | Select the **Authentication Mode**:

- **Machine**—authenticates users using a local account
  or
- **Domain**—authenticates users using Active Directory.
**STEP 3 | Save** your changes.

**Change the Ninja-Mode Password**

To view and modify advanced settings in the ESM Console, you must enter the ninja-mode password. To change the password, use the DB Configuration Tool.

**STEP 1 |** Open a command prompt as an administrator in either of two ways:

- Select **Start** > **All Programs** > **Accessories**, right-click **Command prompt**, and then select **Run as administrator**.
- Select **Start** and, in the **Start Search** box, type **cmd** but do not press **Enter**, yet. Then, to open the command prompt as an administrator, press **Ctrl+Shift+Enter**.

**STEP 2 |** Navigate to the folder that contains the DB Configuration Tool:

```
C:\Users\Administrator> cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server
```

**STEP 3 | (Optional) View the existing server settings:**

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server show
PreventionsDestFolder = \\ESMServer\Quarantine
InventoryInterval = 284
HeartBeatGracePeriod = 300
NinjaModePassword = Password2
```

**STEP 4 |** Specify the new ninja-mode password.

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server NinjaModePassword <password>
```
Export and Import Policy Files

From each rule management page on the ESM Console, you can import and export rules. This enables you to:

- Back up user-defined rules before migrating or upgrading to a new version of the ESM Console.
- Back up user-defined rules before deploying a policy to multiple independent ESM Consoles.
- Import user-defined rules from another ESM Console (running the same version).
- Update your default security policy with the latest recommendations and best practices from Palo Alto Networks.

The ESM Console supports the ability to import both user-defined rules and default security rules.

When you import a policy file that contains multiple types of rules, the ESM Console automatically determines the rule type and distributes the rules to their respective rule management pages. When you export a policy or set of rules, you can only export user-defined rules of the same type. This is because you must select the rules from a single rule management page when you perform the export. When you export rules, the ESM Console saves them to an XML file in the location of your choice.

When you import user-defined rules, the ESM Console appends the rules to the existing policy and assigns each rule a unique ID number. When you install a content update to import the latest default security rules, the ESM Console overwrites the existing rules with the updated policy. When available, you can download the latest default security policy from the Dynamic Updates section of the Support portal.

- User-Defined Rules
- Content Updates

User-Defined Rules

A user-defined rule is a rule that you—or additional administrators with access to the ESM Console—create to manage the Traps security policy and agent settings, or to perform specific actions on the endpoint. A user-defined rule can inherit or override the default security policy.

- Export user-defined rules.
  1. Select the policy management page for the set of rules you are exporting. For example, Policies > Exploit > Protection Modules.
  2. Select the check box next to the rule(s) you want to export or use the check box at the top of the column to select all rules.
  3. From the action menu at the top of the table, select Export Selected. The ESM Console saves the selected rules to an XML file.

- Import user-defined rules.
  1. Select the policy management page for the set of rules you are exporting. If your policy file contains rules of different types (for example, exploit protection and malware protection rules), you can choose any rule management page. For example, select Policies > Exploit > Protection Modules.
  2. Select Import Rules from the action menu at the top of the table.
3. Browse to the policy file, and then click **Upload**.

The ESM Console appends the new rules to the current policy.

---

**Content Updates**

Content updates allow you to easily update your default security policy and settings. Content updates equip the ESM Console with the most up-to-date best practices and threat information for accurate exploit and malware protection and can include changes or additions to:

- Compatibility rules for third-party products and platforms
- Condition objects
- Protected processes
- Restriction settings
- Trusted signers
- Local static analysis logic

These files are packaged in a ZIP file and are hosted on the Support portal.

To manage content updates, use the following workflows:

- **Install a Content Update**
- **Revert to the Previous Content Update**

**Install a Content Update**

Content updates are categorized on the Support portal by ESM version. To update the default policy of the ESM Console, you must use a content update for your ESM version. After you install a content update, the ESM Server transparently distributes any changes to the default policy to your endpoints. This occurs at the next heartbeat communication with the endpoint.

**STEP 1** | Log in to the ESM Console and select **Settings > ESM > Content Updates**.

**STEP 2** | To open the Support portal, do one of the following:
- Select **Support Site** on the ESM Console.
- Open a new browser window and navigate to the **DYNAMIC UPDATES** page on the Support portal.

**STEP 3** | Identify the content update for your ESM version (typically the latest available content update version), and then review the associated Release Notes.

**STEP 4** | Download the content update package to a location that is accessible from the ESM Console.

**STEP 5** | From the ESM Console, select **Update Content**, **Browse** to the content update package, and **Apply**.

*If the content update is older than the current version, the ESM Console displays a warning message.*
After the ESM Console installs the content update, it displays details including version number, release date, and the date on which you installed the content package. You can also view the installed content update version from the footer on each page of the ESM Console. For example, if the ESM Console displays the version as v3.4.0.15481, 5-353, the installed content update version is 5-353.

**Revert to the Previous Content Update**

For convenience, the ESM Console maintains up to two content updates at a time: the current update and the previous update. From the Content Updates page, you can view information about the content updates, roll back to previous content update versions, or install a new (or older) version of a content update. To revert to an older version of a content update, you must download the package from the Support portal and install it as you would a new update.

**STEP 1** | Log in to the ESM Console and select **Settings > ESM > Content Updates**.

**STEP 2** | Review the Release Notes for the previous content update as needed and then Revert.

The ESM Console restores the previous set of default policy rules and distributes them to the endpoints at the next heartbeat communication.
The ESM Console provides information that is useful for monitoring the servers, endpoints, and security policy for your organization. You can monitor the logs and filter the information to interpret unusual behavior on your network. After analyzing a security event, you can choose to create a custom rule for the endpoint or process. The following topics describe how to view and monitor reports on the security health of the endpoints.

- Maintain the Endpoints and Traps
- Use the Endpoint Security Manager Dashboard
- Monitor Security Events
- Monitor the Endpoints
- Monitor the ESM Servers
- View the Rule Summary
- Monitor Forensics Retrieval
Maintain the Endpoints and Traps

On a daily or weekly basis, perform the following actions:

- Examine the Dashboard to verify that the Traps agent is active on all endpoints. See Use the Endpoint Security Manager Dashboard.
- Review Security Events reported by Traps. After analyzing a security event, you might want to do any of the following tasks:
  - Investigate whether the indicators are related to malicious executable files and then use the Agent Query to search for artifacts on endpoints.
  - Disable rules temporarily that interfere with day-to-day work. In cases where a security event does not indicate an attack and is interfering with day-to-day work, you can disable an exploit protection or restriction rule on a specific endpoint. See Exclude an Endpoint from an Exploit Protection Rule.
  - Patch, upgrade, or fix a bug in software that indicates erroneous behavior or a security vulnerability. Patching or upgrading third-party applications or fixing bugs in applications that are developed in-house can reduce the number of security events reported to the ESM Console.
  - Activate protection for an unprotected application. See View, Modify, or Delete a Process.
  - Review post-detection events and take additional action to remediate the endpoint.
- Examine the Monitor pages and investigate reports of crashes and security events.
- If you configured your ESM Console to Collect New Process Information, review unprotected processes and decide whether to enable protection on them. See View, Modify, or Delete a Process.

After a change in the organization or in available Traps software versions, you can:

- Add a newly-installed application to the list of protected processes. See Add a New Protected Process.
- Install Traps on a new endpoint. See Install Traps on Windows Endpoints.
- Upgrade the Traps agent version on endpoints. See Uninstall or Upgrade Traps on the Endpoint.
- Update the agent license on endpoints. See Update or Revoke the Traps License on the Endpoint.
Use the Endpoint Security Manager Dashboard

The Dashboard is the first page that you see when you log into the ESM Console. The Dashboard provides a collection of charts and graphs that display information about the status of the Traps agents that are managed by your Endpoint Security Manager. By default, the ESM Console displays information collected over the past 30 days. To change the display period, see Manage ESM Console Settings.

The following table describes each chart:

<table>
<thead>
<tr>
<th>Dashboard Chart</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVICE STATUS</td>
<td>Displays the status of the Traps agent instances installed on the endpoints by number and percentage. Possible statuses are:</td>
</tr>
<tr>
<td></td>
<td>• Running—The agent is running.</td>
</tr>
<tr>
<td></td>
<td>• Stopped—The agent service has been stopped.</td>
</tr>
<tr>
<td></td>
<td>• Disconnected—The server hasn’t received a heartbeat message from the agent for a preconfigured amount of time.</td>
</tr>
<tr>
<td></td>
<td>• Shutdown—The endpoint has been shut down.</td>
</tr>
<tr>
<td>COMPUTER DISTRIBUTION AND VERSION</td>
<td>Displays the version of the Traps agent instances installed on the endpoints by number and percentage.</td>
</tr>
<tr>
<td>LICENSE CAPACITY</td>
<td>Displays the Traps license utilization for the server and client by number of used and available licenses.</td>
</tr>
<tr>
<td>MOST TARGETED APPLICATIONS</td>
<td>Displays applications that have the highest distribution of preventions.</td>
</tr>
<tr>
<td>MOST TARGETED COMPUTERS</td>
<td>Displays endpoints that have the highest distribution of preventions.</td>
</tr>
<tr>
<td>MOST TARGETED USERS</td>
<td>Displays preventions that have the highest distribution per end user.</td>
</tr>
</tbody>
</table>
Monitor Security Events

Use the Security Events page and tabs to manage alerts and detect new threats.

- Use the Security Events Dashboard
- View the Security Event History on an Endpoint
- Exclude an Endpoint from an Exploit Protection Rule

Use the Security Events Dashboard

Use the Security Events dashboard (Security Events > Summary) to monitor high-level information about security events that occur on the endpoints in your organization. From this view, you can see the number of events that have occurred in the last day, week, or month. The Security Events Dashboard displays both events where exploit attempts were blocked and events that triggered only notifications.

The following table describes the different areas of the dashboard in more detail.

<table>
<thead>
<tr>
<th>Dashboard Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>THREATS</strong></td>
<td>Displays all the threats to protected processes and executable files that have occurred in your network. For convenience, you can click any rule type to view additional details about events of that type. You can also click on the number of events that have occurred to view only those events. For more information, see Manage Security Events.</td>
</tr>
</tbody>
</table>
| **PROVISIONAL MODE**| The Provisional Mode area of the Security Events Dashboard includes a high-level summary of the events that are tied to the following event types:  
  - WildFire Unknown  
  - WildFire Post Unknown Detection  
  - Java  
  - Thread injection  
  - Suspend guard |
Dashboard Component | Description
--- | ---
**Click an event in the Provisional Mode area to jump to a filtered view of the Monitor > Provisional Mode page for events of that type.** 
For more information, see View Provisional Mode Details.

**SECURITY ERROR LOG** | Displays all of the errors and recent issues that Traps reports about the endpoints in your organization. Click any error type or on the number of security errors to view a filtered list of errors from the Monitor > Security Errors Log page. For more information, see View Security Error Log Details.

### Manage Security Events

Select Security Events > Threats to display a list of threats that have occurred in your network. The default view of the threats page includes all prevention and notification events. The menu on the side of the Threats page also provides links to filtered lists of threats by event (Preventions and Notifications) and also by rule type.

The standard details view of the Threats page displays a table of security events with fields displayed along the top. Selecting an event in the Threats table expands the row to reveal additional details about the security event. In addition to viewing details about threat events, you can create and view notes about the event, retrieve log data about the event from the endpoint, or create an exclusion rule to allow the process to run on a particular endpoint.

- **Filter for specific events**
  
  Use the search field to search for users or endpoints, or use the filters at the top of each column to narrow the results.

- **View additional details about the event**
  
  Select the row for the event. The row expands to reveal additional details about the security event.

  _For details on the fields in the security events table, refer to the online help._
• Export events to a comma separated values (CSV) file.
  1. Select the checkbox for each event that you want to export.
  2. Click the action menu ➕, and select **Export Selected**. The ESM Console generates the CSV file containing the selected records.

• Delete events.
  1. Select the checkbox for each event that you want to export.
  2. Click the action menu ➕, and select **Delete Selected**. The ESM Console removes the records from all Security Events pages.

• *(WildFire events only)* View the WildFire Report for an executable file
  From the expanded view of a security event, click **WildFire Report**.

• *(WildFire events only)* Jump to the Hash Control entry for the executable file.
  From the expanded view of a security event, click **Hash Control**.

• Retrieve prevention data from the endpoint.
  From the expanded view of a security event, click **Retrieve Data**. The ESM Console uses the prevention key and trigger information to request data about the prevention event from the agent. After the information is sent to the forensic folder, you can view information about the download from the **Monitor > Data Retrieval** page.

• View administrative notes about the event
  From the expanded view of a security event, click **View Notes** to view notes that you or other administrators entered about the security event. If there are no notes, this option is grayed out.

• Create an administrative note about the event
  From the expanded view of a security event, click **Create Note** to record information about the security event for follow-up at a later time or date.

• *(Exploit events only)* Create a rule to exclude an endpoint from exploit protection.
  From the expanded view of a security event, click **Create Rule** to create an exploit protection rule that excludes the endpoint from the exploit protection rule that prevented the process from running. The rule uses the details from the security event to populate a rule with settings that allow a process to run on a specific endpoint.

**View Provisional Mode Details**

Select **Monitor > Provisional Mode** to display a list of security events related to provisional modules. The provisional modules are configured by default and include WildFireUnknown, WildFirePostUnknownDetection, Java, Thread Injection, and Suspend Guard.
From the **Provisional Mode** page you can view details about the security events, create and view notes about the event, retrieve log data about the event from the endpoint, or create an exclusion rule to allow the process to run on a particular endpoint. By default, the standard details view of the **Provisional Mode** page displays a table of security events with fields displayed along the top. Selecting an event in the Provisional Mode table expands the row to reveal additional details about the security event. You can also export the logs to a CSV file by clicking the menu icon ➕, and selecting **Export Selected**. For details on the fields in the Provisional Mode table, refer to the online help.

**View Security Error Log Details**

Select **Monitor > Security Error Log** to display events related to the behavior of the agent and the security of the endpoint. The events include changes in service such as the start or stop of a service. On rare occasions, the Security Error Log can also show issues encountered during the protection of a process where an injection fails or crashes.

For details on the fields in the Security Error Log table, refer to the online help.

**View the Security Event History on an Endpoint**

When a user launches a process on the endpoint, Traps injects code into the process and activates a protection module known as an Exploit Protection Module (EPM) into the process. The endpoint security policy rules determine which EPMs are injected into each process. During the injection, the process name appears on the console in red. After the injection completes successfully, the console logs the security event on the **Events** tab.

Each security event on the **Events** tab displays the date and time of the event, name of the affected process, and EPM that was injected into the process. Typically, the mode indicates whether or not Traps terminated the process or only notified the user about the event.

**STEP 1 | Launch the Traps Console:**

- From the Windows tray, right-click the Traps icon and select **Console**, or double-click the icon.
- Run CyveraConsole.exe from the Traps installation folder.

The Traps Console launches.
STEP 2 | View the security events:
   1. Select Advanced > Events to display the security events on the endpoint.
   2. Use the up and down arrows to scroll through the list of events.
Monitor the Endpoints

- View Endpoint Health Details
- View Notifications About Changes in the Agent Status
- View the Status of the Agent from the Traps Console
- View the Rule History of an Endpoint
- View Changes to the Security Policy from the Traps Console
- View the Service Status History of an Endpoint
- Remove an Endpoint from the Health Page

View Endpoint Health Details

From the ESM Console, select **Monitor > Agent > Health** to display a list of endpoints in the organization and their corresponding security state.

The standard details view of the Health page displays a table of endpoints with fields displayed along the top. Selecting an endpoint in the Health table expands the row to reveal additional details about the endpoint and actions that you can perform. You can also export the logs to a CSV file by clicking the menu icon and selecting **Export Logs**.

For details on the fields in the **Agent > Health** table, refer to the online help.

View Notifications About Changes in the Agent Status

Use the **Monitor > Agent > Logs** page to view notifications about changes in agent status including starting or stopping services, systems, and processes.

**STEP 1** | From the ESM Console, select **Monitor > Agent > Logs**.

**STEP 2** | To view the table entries, use the paging controls on the top right of each page to view different portions of the table.

**STEP 3** | *(Optional)* To sort the table entries, select the column heading to sort by ascending order. Select the column heading again to sort by descending order.

**STEP 4** | *(Optional)* To filter the table entries, click the filter icon to the right of the column to specify up to two sets of criteria by which to filter the results.

**STEP 5** | *(Optional)* To export the logs to a CSV file, click the menu icon and then select **Export Logs**.
View the Status of the Agent from the Traps Console

The console displays active and inactive services by displaying a ✓ or ✗ to the left of the service type. Select the Advanced tab to display additional tabs along the top of the console. The tabs allow you to navigate to pages that display additional details about security events, protected processes, and updates to the security policy. Usually, a user will not need to run the Traps Console, but the information can be useful when investigating a security-related event. You can choose to hide the tray icon that launches the console, or prevent its launch altogether. For more information, see Hide or Restrict Access to the Traps Console.

<table>
<thead>
<tr>
<th>System Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Exploit Protection</td>
<td>Indicates whether or not exploit prevention rules are active in the endpoint security policy.</td>
</tr>
<tr>
<td>Anti-Malware Protection</td>
<td>Indicates whether or not restriction and/or malware protection modules are enabled in the endpoint security policy.</td>
</tr>
<tr>
<td>Forensic Data Collection</td>
<td>Indicates whether or not WildFire integration is enabled.</td>
</tr>
<tr>
<td>Status tab</td>
<td>Displays the Connection status and level of protection on the endpoint. The Traps console opens to the Status tab by default.</td>
</tr>
<tr>
<td>Events tab</td>
<td>Displays security events that have occurred on the endpoint.</td>
</tr>
<tr>
<td>Protection tab</td>
<td>Displays the processes that the Traps agent protects that are currently running on the endpoint.</td>
</tr>
<tr>
<td>Policy tab</td>
<td>Displays changes to the endpoint security policy including the date and time of the update.</td>
</tr>
<tr>
<td>Verdict Updates tab</td>
<td>Displays changes in verdict for executables that have been opened on the endpoint.</td>
</tr>
<tr>
<td>Settings</td>
<td>Displays language options that you can use to change the language of the Traps Console.</td>
</tr>
<tr>
<td>Check-in now link</td>
<td>Initiates an immediate update of the security policy.</td>
</tr>
<tr>
<td>Connection</td>
<td>Displays the status of the connection between Traps and ESM Server.</td>
</tr>
</tbody>
</table>
### View the Rule History of an Endpoint

The standard details view of the **Health** page displays a table of endpoints with fields displayed along the top. Selecting an endpoint in the Health table expands the row to reveal additional details about the endpoint and allows you to view the rule history of objects in your organization. Each rule in the Agent Policy displays the date and time when Traps applied the rule, source of the policy rule (local or remote), rule name and description, and the current status of that rule.

**STEP 1** | Open the Endpoint Security Manager and select **Monitor > Agent > Health**.

**STEP 2** | Select the row of the endpoint for which you want to view the rule history. The row expands to display further details and actions you can perform.

**STEP 3** | Select **Agent Policy** from the drop-down on the right. The recent status information appears in the Agent Policy and Logs section of the page.

**STEP 4** | Click **Details** to view the full rule history log. The status indicates one of the following:

- **Active**—The rule is active in the endpoint security policy.
- **Historic**—The rule is an older version of a rule that is active in the endpoint security policy.
- **Disabled**—The rule was deactivated in the security policy.

### View Changes to the Security Policy from the Traps Console

The **Policy** tab on the Traps Console displays changes to the endpoint security policy. Each rule displays the unique ID number, name of the rule, date and time that Traps received the updated security policy containing the rule, and description.

> Each rule type has a dedicated management page that you can use to view and manage the rules for your organization. To create a text file containing the active security policy on an endpoint, run the following from a command prompt: `cyveraconsole.exe export (641980)`

`CyveraConsole.exe` creates an XML file in `\programdata\cyvera\logs\ClientPolicy_<date>_<time>.xml` to indicate the date at which the policy was active, for example: `CyveraPolicy_20160831_113415.xml`

**STEP 1** | Do one of the following to launch the Traps Console on the endpoint:

- From the Windows tray, right-click the Traps icon and select **Console**, or double-click the icon.
- Run `CyveraConsole.exe` from the installation folder of the Traps Console.
STEP 2 | View the security policies:
   1. If necessary, click Advanced to reveal additional tabs. Then click the Policy tab to display the protection rules that are running on the endpoint.
   2. Use the up and down arrows to scroll through the list of protection rules.

View the Service Status History of an Endpoint

By default, the standard details view of the Monitor > Agent > Health page displays a table of endpoints with fields displayed along the top. Selecting an endpoint in the Health table expands the row to reveal additional details about the endpoint and allows you to view the status history of the Traps agent on the endpoint. A drop-down on the Agent Policy and Service Status section allows you to display a partial list of Service Status events. From this section you can also view the full service status history log. Each event in the log displays the date and time of the service change, version of Traps that is running on the endpoint and the change in status, either disconnected, running, shutdown, or stopped.

STEP 1 | From the ESM Console select Monitor > Agent > Health.

STEP 2 | Select the row of the endpoint for which you want to view the rule history. The row expands to display further details and actions you can perform.

STEP 3 | Select Service Status from the drop-down on the right. The recent status information appears in the Agent Policy and Logs section of the page.

STEP 4 | Click Details to view the full service status history log.

Remove an Endpoint from the Health Page

The Monitor > Agent > Health page displays a table of all the endpoints that have successfully connected to the Endpoint Security Manager. In situations where you must remove one or more endpoints from the Endpoint Security Manager, such as to clean up duplicates or remove endpoints that are no longer in use, you can use the Delete selected option from the menu at the top of the table.

STEP 1 | From the ESM Console select Monitor > Agent > Health.

STEP 2 | Select the one or more rows of endpoints that you want to delete.

STEP 3 | Select Delete selected from the menu at the top of the Health table. Click OK to confirm the deletion.

The ESM Console removes the endpoint or endpoints from the Health page. Following the heartbeat communication to the endpoint, the connection status on the Traps Console changes to No connection to server.
Monitor the ESM Servers

From the ESM Console you can monitor the health of the ESM Servers in your organization and view changes in their status.

- View the Health of the ESM Servers
- View Notifications About the ESM Server

View the Health of the ESM Servers

Use the Monitor > ESM > Health page to view notifications about changes in the ESM Server health including the number of agents that are connected or disconnected from the server.

By default, the standard details view of the Health page displays a table of servers with fields displayed along the top. Selecting a server in the Health table expands the row to reveal additional details about the server and actions that you can perform. You can also export the logs to a CSV file by clicking the menu icon ➔, and selecting Export Logs.

**STEP 1** | From the ESM Console, select Monitor > ESM > Health.

**STEP 2** | To view the table entries, use the paging controls on the top right of each page to view different portions of the table.

**STEP 3** | (Optional) To sort the table entries, select the column heading to sort by ascending order. Select the column heading again to sort by descending order.

**STEP 4** | (Optional) To filter the table entries, click the filter icon ▼ to the right of the column to specify up to two sets of criteria by which to filter the results.

**STEP 5** | (Optional) To export the logs to a CSV file, click the menu icon ➔, and then select Export Logs.

**STEP 6** | (Optional) To view a list of agents that are connected to the ESM Server, expand the row for the server, and then click Agent List next to the connected or disconnected field. If there are no agents, this option is grayed out.

View Notifications About the ESM Server

The Monitor > ESM > Logs page displays notifications about and actions initiated from the ESM Server(s) including administrative changes, license changes, server management changes, policy management changes, and WildFire changes. For details on the fields in the ESM > Logs table, refer to the online help.

**STEP 1** | From the ESM Console, select Monitor > ESM > Logs.

**STEP 2** | To view the table entries, use the paging controls on the top right of each page to view different portions of the table.

**STEP 3** | (Optional) To sort the table entries, select the column heading to sort by ascending order. Select the column heading again to sort by descending order.

**STEP 4** | (Optional) To filter the table entries, click the filter icon ▼ to the right of the column to specify up to two sets of criteria by which to filter the results.
STEP 5 | (Optional) To export the logs to a CSV file, click the menu icon = , and then select Export Logs.
View the Rule Summary

Each rule summary and management page displays active and inactive rules for your organization and has tools that you can use to manage the rules. To view a rule summary page or find specific rules:

**STEP 1** | From the ESM Console, select the rule management page for that rule type, for example **Policies > Exploit > Protection Modules**.

**STEP 2** | To view the table entries, use the paging controls on the top right of each page to view different portions of the table.

**STEP 3** | *(Optional)* To sort the table entries, select the column heading to sort by ascending order. Select the column heading again to sort by descending order.

**STEP 4** | *(Optional)* To filter the table entries, click the filter icon ▼ to the right of the column to specify up to two sets of criteria by which to filter the results.

**STEP 5** | *(Optional)* To expand a rule entry, click the expansion arrow on the right side of the rule. From the expanded view, you can view further rule details or take any of the actions to manage a rule. See **Save Rules**.
Monitor Forensics Retrieval

The Monitor > Forensics Retrieval page displays information about forensic data files and allows you to manage the data files from a central location. Examples of data files that can be displayed on the Forensics Retrieval page include:

- ESM Tech Support Files
- Logs from the agent
- WildFire updates
- Memory dump collection

You can sort the table entries in ascending order by selecting the column heading. Select the heading again to sort the table entries in descending order. To narrow your results, click the filter icon to the right of the column and specify up to two sets of criteria. You can also export the logs to a CSV file by clicking the menu icon and selecting Export Logs. For details on the fields in the Forensics Retrieval page, refer to the online help.
Getting Started with Rules

The following topics describe the basic components and processes associated with each rule:

> Endpoint Policy Rule Concepts
> Policy Rule Types
> Common Rule Components and Actions
Endpoint Policy Rule Concepts

- Policy Rule Types
- Policy Enforcement
Policy Rule Types

A complete endpoint security policy comprises policies that target specific methods of protection. The rules that make up each of these policies enable you to enforce protection, manage Traps settings, and take action on your endpoints. You can configure rules that target specific objects or that take effect when they match specific conditions and, together, these rules help to secure the endpoints in your organization.

The following table describes the types of policies you can configure in the ESM Console:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware protection</td>
<td>Malware protection rules use protection modules to block common behavior initiated by malicious executable files. Each rule in the malware protection policy specifies the type of protection module used to block suspicious actions. The rule can also include a whitelist that specifies exceptions to the rule. For more information, see Malware Protection Rules.</td>
</tr>
<tr>
<td>Exploit protection</td>
<td>Exploit protection rules determine the method of protection for processes that run on your endpoints. Each rule in the exploit prevention policy specifies the type of protection modules used to protect processes. For more information, see Exploit Protection Rules.</td>
</tr>
<tr>
<td>Restrictions</td>
<td>Restriction rules limit the scope of an attack by specifying where and how executable files can run that are launched on endpoints. For more information, see Restriction Rules.</td>
</tr>
<tr>
<td>WildFire</td>
<td>WildFire rules enable pre- and post-prevention analyses of executable files by sending executable file hashes and, optionally, hashes for unknown files, as well, to the WildFire cloud. For more information, see Configure a WildFire Rule.</td>
</tr>
<tr>
<td>Forensics</td>
<td>Forensics rules enable you to set preferences about memory dump and forensic file collection. For more information, see Forensics Rules.</td>
</tr>
<tr>
<td>Agent settings</td>
<td>Agent settings rules enable you to change the values of Traps agent settings related to logging, heartbeat frequency, and console accessibility. For more information, see Traps Agent Settings Rules.</td>
</tr>
<tr>
<td>Action</td>
<td>Action rules allow you to perform administrative activities on endpoints. The one-time management actions include uninstalling and upgrading Traps, updating licenses, protecting the Traps software, and clearing data files. For more information, see Traps Action Rules.</td>
</tr>
</tbody>
</table>

Policy Enforcement

Traps evaluates rules based on the type of policy associated with the rule. Exploit protection, malware protection, and restriction rules are evaluated only when a process or executable file launches and when the rule also matches the specified Target Objects, Conditions, and settings. A target object can be any user, group, organizational unit, or computer that appears in Active Directory or any endpoint on which Traps is installed. The Endpoint Security Manager identifies endpoints according to messages that Traps sends to the server. A condition can be an exact match of a file, a file and the file version, or a registry path that must
exist on the endpoint. You can also define a condition for a specific version of an executable file defined in
the file path.

At regular heartbeat intervals, the Traps agent requests the latest endpoint security policy from the ESM
Server. You can define the frequency of the security policy updates on the endpoint by tuning the heartbeat
setting. From the Traps Console, you can also manually retrieve the latest security policy. Traps applies
agent settings or action policy rules when the endpoint receives the security policy update and a rule
matches the Target Objects, Conditions, and settings of the endpoint.

Traps evaluates each rule in the security policy sequentially by ID number: the bigger the ID number, the
higher the priority of the rule. Recently created or modified rules are assigned a higher ID number and are,
therefore, evaluated first. Unlike Palo Alto Networks firewalls, which evaluate rules hierarchically, Traps
evaluates all rules in the endpoint security policy sequentially.

If multiple rules contain the same core configuration (for example, multiple rules configured for the same
malware protection module), Traps determines which rule takes precedence to avoid rule conflicts. To
determine the precedence, Traps considers rule specificity and identification number. If a rule has a
narrower scope than another rule, such as an exploit protection rule configured for a specific process versus
an exploit protection rule configured for all processes, the rule with the narrower (more specific) scope
takes precedence. If the rules have the same scope, Traps gives precedence to the rule with the bigger
identification number (which indicates a more recent creation date).
Common Rule Components and Actions

Each type of rule has a specific set of required and optional fields that you can customize to meet the needs of your organization's security policy.

The following table describes the common steps for creating an endpoint security policy rule.

<table>
<thead>
<tr>
<th>Manage Rules</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the settings and actions that are specific to the rule type.</td>
<td>For more details on the specific settings required for each rule type, see:</td>
</tr>
<tr>
<td></td>
<td>• Manage Malware Protection Rules</td>
</tr>
<tr>
<td></td>
<td>• Manage Exploit Protection Rules</td>
</tr>
<tr>
<td></td>
<td>• WildFire Integration</td>
</tr>
<tr>
<td></td>
<td>• Manage Restrictions on Executable Files</td>
</tr>
<tr>
<td></td>
<td>• Manage Traps Action Rules</td>
</tr>
<tr>
<td></td>
<td>• Manage Agent Settings Rules</td>
</tr>
<tr>
<td></td>
<td>• Manage Forensics Rules and Settings</td>
</tr>
<tr>
<td>Add activation conditions to the rule—conditions that the endpoint must fulfill for a rule to be applied.</td>
<td>Conditions</td>
</tr>
<tr>
<td>Define the target objects (users, computers, organizational units, groups, and endpoints).</td>
<td>Target Objects</td>
</tr>
<tr>
<td>Provide a descriptive name for the rule.</td>
<td>Name or Rename a Rule</td>
</tr>
<tr>
<td>Save and optionally activate the rule.</td>
<td>• Save Rules</td>
</tr>
<tr>
<td></td>
<td>• Manage Saved Rules</td>
</tr>
<tr>
<td>Back up or restore rules.</td>
<td>Export and Import Policy Files</td>
</tr>
<tr>
<td>Filter the rules shown on the page.</td>
<td>Filter Rules</td>
</tr>
<tr>
<td>View the default policy rules.</td>
<td>Show or Hide the Default Policy Rules</td>
</tr>
<tr>
<td>Disable or enable all protection rules.</td>
<td>Disable or Enable All Protection Rules</td>
</tr>
</tbody>
</table>

Conditions

Rule activation conditions are conditions that the endpoint must fulfill to apply that rule on the endpoint. For each condition, you can specify either an executable file path, an executable file path and file version, or a registry path that must exist on the endpoint.

- Define Activation Conditions for a Rule
- Include or Exclude Endpoints Using Conditions
- Delete or Modify a Rule Condition
Define Activation Conditions for a Rule

Use the following workflow to create a new activation condition for a rule.

STEP 1 | Select Settings > Conditions. The Conditions page displays the unique ID number, Name, Description, and Path (if applicable) for each condition.

STEP 2 | Add a new condition.

STEP 3 | Enter the Name and Description of the condition.

STEP 4 | Configure the type of condition to match the path of a specific executable file, to match a specific version or range of versions for a specific executable file, or to match a specific registry key:

- To match a specific executable file (or to match a specific version of an executable file), specify the full Path of an executable file that exists on the endpoint. Optionally, you can use system variables in the path. For example, specify `%windir%\system32\calc.exe` to apply the rule if the calculator executable file is run from this location.
- If you specified an executable file in the Path field, you can also set a match condition for a Version or range of versions of that executable file. If you specify a Version value, Traps will only apply the rule if the executable is run from the location specified in the Path field and also matches the Version value. By default, the condition matches any version of the file. To narrow the number of versions, select one of the following Version Comparison options and then enter a Version number.

  The Version value must follow the standard Windows version convention and be no longer than four segments long (for example, 4.30.200.100). To match versions longer than four segments long, use Regex.

  - **Equal**—Match an exact version.
  - **Greater**—Match any version that is equal to or greater than the specified version.
  - **Lesser**—Match any version that is equal to or lesser than the specified version.
  - **Between**—Match any version inclusive of and between two values. For example, to set a condition that matches Internet Explorer versions between and including versions 8 and 9, enter `C:\Program Files\Internet Explorer\iexplore.exe` in the Path field, select Version Comparison: Between, and enter 8 and 9 in the Version fields.
  - **Regex**—Match a version using .NET Framework 4 regular expressions.


For example, to match any version of 3.1.x including 3.1, use the following regular expression: `3\.1\(\[0-9\]+\)`. To match only versions 3.1.0-3.1.9 use: `3\.1\(\[0-9\]\)`. To match only version 3.2 and 3.4, use: `3\.2\[24\]`

- Specify a full Registry Path for a registry entry, beginning with one of the following: LocalMachine, ClassesRoot, Users, PerformanceData, CurrentConfig, or DynData.

  You cannot specify CurrentUser registry paths because Traps runs as the local system.

Traps will only apply the rule if the endpoint contains the specified path in its registry. You can also configure a specific registry Key or Data value (String and DWord only) as a match condition.

For example, to apply a rule on endpoints that have IPv6 enabled, configure a condition that matches the following registry settings:
• Registry Path: LocalMachine\SYSTEM\CurrentControlSet\services\TCP/IP6\Parameters\EnableICSIPv6
• Key: DisabledComponents
• Data: 0

STEP 5 | Save the condition.

You can use the condition as a match criteria to either include or exclude endpoints from receiving a rule. See Include or Exclude Endpoints Using Conditions.

Include or Exclude Endpoints Using Conditions

By configuring conditions, you can activate rules for only those endpoints that match the condition. For example, consider a condition that matches Windows XP client systems. When you add that condition to an include list, the rule will apply only if the client system is running Windows XP. Conversely, if you add that same condition to an exclude list, the rule will apply to all client systems except those running Windows XP. After you add a condition to a list (include or exclude), you cannot use it in the other list.

Use the following workflow to include or exclude an endpoint from a rule using conditions.

STEP 1 | From the rule configuration page, select the Conditions tab.

STEP 2 | Select a condition and Add it to the include or exclude list. To select multiple conditions, press and hold the Ctrl key while selecting.

STEP 3 | Configure the rule settings and then Save or Apply the rule (see Save Rules).

Delete or Modify a Rule Condition

Rule activation conditions are conditions that the endpoint must fulfill for a rule to apply to that endpoint. After you create a condition, you can delete or modify it from the Conditions page.

STEP 1 | Select Settings > Conditions. The Conditions page displays the unique ID number, Name, and Description for each condition.

STEP 2 | Select the condition that you want to modify or delete.

STEP 3 | Do either of the following.

• Click Delete to discard the condition.
• Modify the condition settings, and then Save the changes.

Target Objects

Target objects define the scope of a rule and the endpoints to which a rule applies. An object can be one of the following:

<table>
<thead>
<tr>
<th>Target Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>A user defined in Active Directory.</td>
</tr>
<tr>
<td>Groups</td>
<td>A user group defined in Active Directory.</td>
</tr>
<tr>
<td>Computers</td>
<td>The name of a computer or mobile device defined in Active Directory.</td>
</tr>
<tr>
<td>Target Object</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Organizational Unit</strong></td>
<td>A subdivision within Active Directory into which you can place users, groups, computers, and other organizational units.</td>
</tr>
<tr>
<td><strong>Existing Endpoints</strong></td>
<td>A computer or mobile device on which the Traps agent is installed. The Endpoint Security Manager identifies existing endpoints by communication messages it receives from Traps agents.</td>
</tr>
</tbody>
</table>

For objects defined in Active Directory, the ESM Console provides autocompletion as you type.

*Computer names may be offered as autocompletions even if they are not presently running Traps.*

You can apply rules to all objects, to selected objects, or to all objects except those in the Exclude list. Rules that you define for users and groups will apply to those users and groups, regardless of the endpoint on which they log in.

**Name or Rename a Rule**

The ESM Console automatically generates the rule name and description based on the rule details and time of creation. To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter your own rule name and description.

*The rule that is modified or edited most recently takes precedence over older rules of the same type. As a result, changing the name of a rule changes the modification date for the rule and can cause the edited rule to override older rules.*

*The rule description is a good place to record the business reasons for the creation of a rule. For example, you might include an incident identification number or a link to a help desk ticket.*

**Save Rules**

To save a rule, you must complete all required fields for that rule type. Tabs with required fields are indicated by a red tab background.

Complete the required fields before attempting to save or modify a rule. After specifying the required fields for a rule, you can select one of the following actions:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save</strong></td>
<td>Save the rule without activating it. The status of the rule is shown as <strong>Inactive</strong>, and you can activate it later. This option is only available for inactive, new, or cloned default rules.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Apply</strong></td>
<td>Save the rule and activate it immediately. The ESM Server sends the updated rule at the next heartbeat communication with the Traps agent. However, you can trigger a policy update by clicking <strong>Check-in now</strong> in the Traps console on an endpoint.</td>
</tr>
</tbody>
</table>

### Manage Saved Rules

After saving the rule, the name and description appear in the appropriate system logs and tables.

Select the rule to view details and perform any of the following actions:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Duplicate</strong></td>
<td><em>(Action rules only)</em> Create a new rule from an existing rule.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>Discard the rule; the rule is removed from the system.</td>
</tr>
<tr>
<td></td>
<td>To delete multiple rules at the same time, select the rules and then select <strong>Delete Selected (non-Default)</strong> from the action menu ➔ at the top of the table.</td>
</tr>
<tr>
<td><strong>Activate/Deactivate</strong></td>
<td>If the rule was previously saved but not applied, you can <strong>Activate</strong> the rule to add it to the current security policy. If the rule is active, you can <strong>Deactivate</strong> it to remove the rule from the current security policy but not from the system. To activate or deactivate multiple rules at the same time, select the rules and then select <strong>Activate Selected</strong> or <strong>Deactivate Selected</strong> from the menu ➔ at the top of the table. To disable or enable all exploit, malware, or forensics rules, see <strong>Disable or Enable All Protection Rules</strong>.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Edit the rule definition. Selecting this option opens the rule configuration dialog and allows you to change the rule definition. For more information, see <strong>Create an Exploit Protection Rule</strong>.</td>
</tr>
<tr>
<td><strong>Import Rules/Export Selected</strong></td>
<td>From the action menu ➔ at the top of the table, you can import rules or export selected rules. Exporting rules saves the selected rules to an XML file. For more information, see <strong>Export and Import Policy Files</strong>.</td>
</tr>
<tr>
<td><strong>Show Default Rules/Hide Default Rules</strong></td>
<td>From the action menu ➔ at the top of the table, you can expand the default rules or hide default rules. Select the rule to view additional information about the rule. For more information, see <strong>Show or Hide the Default Policy Rules</strong>.</td>
</tr>
<tr>
<td><strong>Clone</strong></td>
<td>When you show default rules and then select a rule, the ESM Console displays additional details about the rule settings and an option to <strong>Clone</strong> the rule. Cloning enables you to create a new rule that overwrites the default policy settings. For more information, see <strong>Show or Hide the Default Policy Rules</strong>.</td>
</tr>
</tbody>
</table>
Filter Rules

Each rule summary and management page in the ESM Console displays details about the rules that define your organization’s security policy. To narrow the number of rules that the ESM Console displays, you can filter the rules using the filter control at the top of each column. Use the filter control to define either one or two values to filter on rule status, rule name, rule description, or modification date.

The operators that are available for each column depend on the column type. For example, you can filter columns that display text using any of the following operators to search for a string value: *Is equal to*, *Is not equal to*, *Starts with*, *Contains*, *Does not contain*, or *Ends with*. For columns that display a date, you can filter for a specific date or a date range using any of the following operators: *Is equal to*, *Is not equal to*, *Is after or equal to*, *Is after*, *Is before or equal to*, or *Is before*.

The ESM Console identifies columns that have active filters with an applied filter icon and a blue background. To remove the filter, click the icon and then select **Clear**.

The following table shows the columns, operators, and values that you can use to filter the rules.

<table>
<thead>
<tr>
<th>Column</th>
<th>Operators</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Status</td>
<td>• Is equal to</td>
<td>• Pending—Not used.</td>
</tr>
<tr>
<td></td>
<td>• Is not equal to</td>
<td>• Active—Applied rules.</td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
<td>• Inactive—Deactivated rules.</td>
</tr>
<tr>
<td></td>
<td>• Contains</td>
<td>• Historic—Deleted rules.</td>
</tr>
<tr>
<td></td>
<td>• Does not contain</td>
<td>• Migrated—Not used.</td>
</tr>
<tr>
<td></td>
<td>• Ends with</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>• Is equal to</td>
<td>&lt;string&gt;</td>
</tr>
<tr>
<td></td>
<td>• Is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Does not contain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ends with</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>• Is equal to</td>
<td>&lt;string&gt;</td>
</tr>
<tr>
<td></td>
<td>• Is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Starts with</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Does not contain</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ends with</td>
<td></td>
</tr>
<tr>
<td>Date Modified</td>
<td>• Is equal to</td>
<td>&lt;mm/dd/yyyy&gt;</td>
</tr>
<tr>
<td></td>
<td>• Is not equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is after or equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is after</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is before or equal to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is before</td>
<td></td>
</tr>
</tbody>
</table>
Disable or Enable All Protection Rules

If the endpoint protection security policy is causing issues for endpoints in your organization, you can quickly disable all active policy rules including the default policy rules. Disabling protection effectively removes all restrictions and halts the following tasks:

- Traps injection into all processes that run in the future
- Validation against WildFire
- Further data collection

Modifying security policy rules while all protection is disabled has no effect until protection is re-enabled. After disabling protection and resolving the issues, you can restore all the policy rules at the same time by enabling all protection. (Enabling protection does not activate rules that were previously deactivated.)

In a scenario where you need to disable only a single rule or small group of rules, you can individually select and deactivate those rules from the rule management page specific to that rule type.

**STEP 1** | From the ESM Console, select any rule management page, such as Policies > Malware > Restrictions.

**STEP 2** | Do either of the following:

- To disable protection, click Disable All Protection. The ESM disables all rules and sends the updated security policy to the endpoints at the next heartbeat communication with the Traps agents.
- To enable protection, click Enable All Protection. The ESM re-enables all rules and sends the updated endpoint protection security policy to the endpoints at the next heartbeat communication with the Traps agents.

Show or Hide the Default Policy Rules

The Endpoint Security Manager security policy comes preconfigured with rules that protect against attacks that leverage common software vulnerabilities, exploits, and attack vectors.

When configuring new rules, you can inherit the default behavior or you can override settings as needed to customize your organization’s security policy.

To reduce the number of rules you see in your security policy, the default rules are collapsed under a single default policy.

- **Hide/Show Default Rules**
  - To expand and view the default policy rules, select Show Default Rules from the action menu at the top of the page.
  - To collapse the list of rules, use the Hide Default Rules action.

- **Modify a Default Rule**
  To override a default rule, you can clone the rule and edit the settings. In the case of similar rules, the more recent rule takes precedence over the older rule.
  1. Select Show Default Rules from the action menu at the top of the page.
  2. Select the desired rule to view additional details.
  3. Clone the rule and edit the settings as desired.
  4. Save or Apply the rule when finished.
Malware Protection

> Malware Protection Concepts
> Malware Protection Policy Best Practices
> Malware Protection Flow
> WildFire Integration
> Manage Hashes for Executable Files
> Manage Restrictions on Executable Files
> Manage Malware Protection Rules
Malware Protection Concepts

- ESM Forwarding
- Verdicts
- Verdict Caches
- File Type Analysis

ESM Forwarding

The Endpoint Security Manager (ESM) forwards unknown samples for WildFire analysis based on the configured WildFire settings (Settings > ESM > WildFire). You can also configure additional behavior for different groups of users by configuring WildFire rules (Policies > Malware > WildFire). For samples that Traps reports, the agent first checks its local cache of hashes to determine if it has an existing verdict for that sample. If not, Traps queries the ESM to determine if WildFire has previously analyzed the sample. If the sample is identified as malware, it is blocked. If the sample remains unknown after comparing it against existing WildFire signatures, the ESM forwards the sample for WildFire analysis. For more information, see Malware Protection Flow.

Verdicts

WildFire delivers verdicts to identify samples it analyzes as safe, malicious, or unwanted (grayware is considered obtrusive but not malicious):

- **Benign**—The sample is safe and does not exhibit malicious behavior.
- **Malicious**—The sample is malware and poses a security threat. Malware can include viruses, worms, Trojans, Remote Access Tools (RATs), rootkits, and botnets. For files identified as malware, WildFire generates and distributes a signature to prevent against future exposure to the threat.
- **Grayware**—The sample does not pose a direct security threat, but might display otherwise obtrusive behavior. Grayware typically includes adware, spyware, and Browser Helper Objects (BHOs).

Verdict Caches

Traps stores hashes and the corresponding Verdicts for all executable files that open on the endpoint in its local cache. The local cache is stored in the C:\ProgramData\Cyvera\LocalSystem folder on the endpoint and scales in size to accommodate the number of unique executable files opened on the endpoint. When service protection is enabled (see Manage Service Protection), the local cache is accessible only by the Traps agent and cannot be changed.

Each time an executable file attempts to run, the Traps agent performs a lookup in its local cache to determine if a verdict already exists. If known, the verdict is either the official WildFire verdict or manually set as an administrative hash control policy. Verdicts with an administrative hash control policy take precedence over any additional verdict analysis.

If the executable file is unknown in the local cache, the Traps agent then queries the ESM Server for the verdict. The Endpoint Security Manager stores verdicts for all executable files that have been opened on the endpoints across your organization in its server cache which is stored in the ESM database. When the ESM Server receives a verdict request it performs a lookup in its server cache to determine the verdict. The ESM Server responds with the verdict at the next heartbeat communication with the Traps agent that requested the verdict.

If the executable file is unknown in the server cache, the ESM Server then queries WildFire and optionally submits the file for analysis.
File Type Analysis

You can configure your ESM to forward samples to WildFire for analysis. A sample can be any executable file including (but not limited to) .exe and Microsoft Windows screensaver files.

For details on enabling the ESM to forward samples to WildFire, see Set Up the ESM to Communicate with WildFire.
Malware Protection Policy Best Practices

The key principle when defining a malware protection policy is to minimize the chance of infection from known and unknown malware. To achieve this goal, the best practice malware protection policy uses WildFire rules that enable Traps to identify and block all known threats and send unknown files for analysis and identification by WildFire. In addition, the best practice malware protection policy enables Traps to take advantage of built-in mechanisms to analyze unknown executable files and determine the likelihood of malware. Consider the following recommendations when creating a malware protection policy:

- **Enable WildFire integration** to allow Traps to evaluate executable files based on their WildFire verdicts. WildFire integration is automatically enabled in the default policy. Therefore, if you need to create new WildFire rules, ensure that WildFire Activation is On. See Configure a WildFire Rule.

- **Block the execution of malware.** The easiest way to prevent malware from causing harm to your endpoints is to block its execution. To do this, the Action in the WildFire policy must be set to Prevention. Because the default policy configures this setting, we recommend that you leave the default setting, or if you need to create new rules, inherit the action from the default policy. See Configure a WildFire Rule.

- **Enable Traps to submit unknown executable files** to the ESM Server and enable the ESM Server to send those samples to WildFire for analysis. By submitting the samples, you take advantage of advanced WildFire threat intelligence which enables analysis and identification of zero-day malware. WildFire also makes information about newly-discovered executable files available globally to other ESMs (upon query) and to Palo Alto Networks firewalls (within minutes). This enables you and other Palo Alto Networks customers to transform unknown samples to known samples thus reducing the time spent determining the nature of the unknown executable file. Because the default policy configures this setting, no additional action is required to enable this functionality. However, if you need to create new rules, ensure that you enable Upload files for WildFire analysis. See Set Up the ESM to Communicate with WildFire.

- **Enable Traps to perform local analysis** on unknown executable files to determine if they are likely to be malware. Local analysis uses a statistical model that was developed using machine learning on WildFire threat intelligence. When enabled, local analysis uses the model to issue a local verdict for the file. Traps simultaneously queries the ESM Server for a verdict for the unknown executable but can use the local analysis verdict until the ESM Server responds with either an official WildFire verdict or administrative hash control policy. Because the default policy configures this setting, no additional action is required to enable this functionality. However, if you need to create new rules, ensure that you enable Local Analysis. See Local Static Analysis.

- **Install the latest content update.** Each content update packages the latest Palo Alto Networks threat intelligence into a default security policy file. The content update can include changes to the list of trusted signers, local analysis model, compatibility rules, and default rule configuration settings. By installing the latest content update, you can ensure that your endpoints take advantage of this threat intelligence. See Content Updates.
Malware Protection Flow

To protect the endpoint from malicious and unknown executable files, the malware prevention engine employs three methods of protection:

- WildFire analysis of known and unknown executable files
- Restriction policy rules that examine the source of the file
- Malware protection modules that target behaviors commonly initiated by malicious processes

**Phase 1: Evaluation of Hash Verdicts**

When WildFire is enabled (see Set Up the ESM to Communicate with WildFire), Traps calculates a unique hash using the SHA-256 algorithm for every executable file that attempts to open on the endpoint. Depending on the WildFire features that you enable in your WildFire rule, the Traps WildFire module performs additional analysis to determine whether an unknown executable is malicious or benign. Traps can also submit unknown executable files to the ESM Server for analysis by WildFire.

The evaluation stages are described in more detail in the following sections:

- Administrative Hash Control Policy
- Trusted Signers
- WildFire Verdict
- Local Static Analysis

**Administrative Hash Control Policy**

The administrative hash control policy (also referred to as a verdict override or simply hash control policy), enables you to change the verdict for a specific executable file without affecting your WildFire policy.
integration settings. The hash control policy is evaluated first and takes precedence over all other methods to determine the hash verdict.

From the ESM Console, you can configure a verdict override for any of the following situations:

- You want to block a file that has a benign verdict.
- You want to allow a file that has a malware verdict. In general, we recommend that you only override the verdict for malware after you use available threat intelligence resources—such as WildFire and AutoFocus—to determine that an executable file is not malicious.
- You want to specify verdict for an executable file that has not yet received an official WildFire verdict

After you configure a hash control policy, the ESM Server distributes it at the next heartbeat communication with any endpoints that have previously opened the executable file.

When an executable file launches on the endpoint, Traps first evaluates whether a hash control policy is configured for the file. The hash control policy indicates that Traps should either treat the executable file as malware or as a benign executable file. If the case of an executable file with a benign verdict, the file must still pass evaluation by restriction rules (see Phase 2: Evaluation of the Restriction Policy) and malware protection rules (see Phase 3: Evaluation of the Malware Protection Policy) before Traps permits it to open.

If a hash control policy is not configured for the file, Traps next employs the WildFire module to determine the verdict. The WildFire module uses a three-step evaluation process in the following order to determine the verdict: Trusted Signers, WildFire Verdict, and then Local Static Analysis.

## Trusted Signers

Legitimate software is often signed by a trusted signer to signify that the software has not been altered or tampered with. Palo Alto Networks regularly reviews and makes changes to the list of trusted signers and makes the list available with the default security policy. Any updates to the list of trusted signers are made available with content updates that you can obtain from the Support portal (for more information, see Content Updates).

When a user attempts to open an unknown executable file for which a hash control policy does not exist, the WildFire module begins the verdict evaluation process by verifying whether an executable file is signed by a trusted signer.

If the executable file is signed by a trusted signer, the file is considered benign and is locally exempt from additional WildFire verification and local analysis. As long as execution restrictions and malware protection rules do not apply to the executable file, Traps permits it to open. If Traps blocks a file that is signed by a trusted signer (for example, if the file was signed by a trusted signer but violated a restriction rule), the ESM Console displays the signer information in the new Source Signers field in the security event details.

If the executable file is not signed by a trusted signer, Traps next evaluates the official WildFire Verdict.

> In very rare occasions, WildFire can return a malicious file verdict for an executable file that is signed by a trusted signer. If this rarity occurs, the ESM Console reports a Post Detections event. You can review these events in the Post Detections area of the Security Events page. To override the default behavior, which permits the executable file to run, configure an administrative hash control policy to block the file.

## WildFire Verdict

If an executable file is not signed by any Trusted Signers, the Traps agent performs a hash verdict lookup to determine if a verdict already exists in its local cache.

If the executable file has a malware verdict, Traps reports the security event to the Endpoint Security Manager and, depending on the configured behavior for malicious files, Traps then does one of the following:

- Blocks the malicious executable file
• Notifies the user about the file but still allows the file to execute
• Logs the issue without notifying the user and allows the file to execute.

If the verdict for a hash indicates that the associated file is benign, Traps moves on to the next stage of evaluation (see Phase 2: Evaluation of the Restriction Policy).

If the hash does not exist in the local cache or has an unknown verdict, Traps performs Local Static Analysis.

**Local Static Analysis**

Local analysis enables Traps to examine hundreds of characteristics of an unknown executable file to determine if it is likely to be malware. The local analysis module uses a statistical model that was developed using machine learning on WildFire threat intelligence.

Traps performs local analysis only on unknown executable files and enables Traps to issue a local verdict (benign or malicious) while the endpoint is offline or the ESM Server is unreachable. Traps can rely on the local analysis verdict until it receives an official WildFire verdict or updated hash control policy.

Local analysis is enabled by default in the WildFire policy. Because local analysis always returns a verdict for an unknown executable file, enabling the option to Block unknown files only applies to agents for which local analysis is not enabled or for agents running versions earlier than Traps 3.4. To change the default settings, clone the default WildFire rule and disable Local Analysis (not recommended). For more information, see Configure a WildFire Rule.

**Phase 2: Evaluation of the Restriction Policy**

When a user or machine attempts to open an executable file, Traps first evaluates the hash verdict for the executable file as described in Phase 1: Evaluation of Hash Verdicts. If the executable file is not malicious, Traps next verifies that the executable file does not violate any restriction rules. For example, you might have a restriction rule that blocks unsigned executable files or that blocks executable files launched from network locations. If a restriction rule applies to an executable file, Traps blocks the file from executing and reports the security event to the Endpoint Security Manager and, depending on the configuration of each restriction rule, Traps can also notify the user about the prevention event.

If no restriction rules apply to an executable file, Traps permits the file to execute and next evaluates the rules that protect the endpoint from malicious behavior (see Phase 3: Evaluation of the Malware Protection Policy).

**Phase 3: Evaluation of the Malware Protection Policy**

If an executable file is not blocked by both the WildFire (as described in Phase 1: Evaluation of Hash Verdicts) and the restriction policy (as described in Phase 2: Evaluation of the Restriction Policy), Traps permits the file to execute. If the executable file exhibits malicious behavior as determined by your malware prevention policy, Traps stops the file from executing and prevents the malicious behavior from continuing. For example, consider a case where you have a Thread Injection rule that prevents processes from creating remote threads. If the executable file launches and then attempts to create remote threads, Traps blocks the executable file from continuing to run and reports the security event to the Endpoint Security Manager.
WildFire Integration

WildFire is the Palo Alto Networks sandbox solution for analyzing unfamiliar files—including unknown executable files. WildFire contains verdicts for all scrutinized files: benign in the case of a safe file and malicious in the case of malware. The WildFire integration with Traps is an optional service that incorporates WildFire analysis into your Traps endpoint solution.

When a user or a machine tries to open an executable file on the endpoint, Traps calculates a unique identifier (known as a hash) using the SHA-256 algorithm. The ESM Server then checks it against the WildFire database. If WildFire confirms that a file is known malware, Traps blocks the file and notifies the Endpoint Security Manager (for more information, see Manage Hashes for Executable Files).

- Set Up the ESM to Communicate with WildFire
- Configure a WildFire Rule

Set Up the ESM to Communicate with WildFire

WildFire integration is enabled by default; however, you must set up the ESM to communicate with WildFire.

STEP 1 | From the ESM Console, select Settings > ESM > WildFire.

![WildFire Configuration]

STEP 2 | Enable WildFire communication settings:

- Select Allow External Communication with WildFire to enable the ESM to check hashes with WildFire.
- Select Allow Upload Executable Files to WildFire to enable the ESM to send files to WildFire for analysis. Clearing this upload option enables the ESM Server to check verdicts with WildFire but not send files for analysis.

STEP 3 | In the Unknown Verdicts Recheck Interval field, enter the frequency (in minutes) at which the ESM Server resubmits hashes to WildFire for unknown files. A file can have an unknown verdict if it is the first time an endpoint submits the hash to the server or if WildFire has not, yet, analyzed or finished analyzing the file (range is 1 to 20,160; default is 30).

STEP 4 | In the Known Recheck Verdict Interval field, enter the frequency (in minutes) at which the ESM Server rechecks with WildFire for the value of known benign or malicious hashes (range is 1 to 20,160; default is 1,440).
STEP 5 | In the **Upload Retry Interval (Minutes)** field, enter the frequency (in minutes) at which the ESM Server attempts to re-upload any files that did not upload to WildFire successfully (range is 1 to 20,160; default is 1,440).

STEP 6 | The ESM Server queries WildFire every 24 hours or as specified in **4** to determine which verdicts, if any, have changed within the last 30 days (default). You can change how far back the ESM Server queries for changed verdicts by specifying a value from 1 to 30 in the **Verdict change check interval** field. For example, specifying a value of 15 means that the ESM Server will query for verdicts that have changed within the last 15 days.

STEP 7 | Enter the WildFire cloud web address ([https://wildfire.paloaltonetworks.com](https://wildfire.paloaltonetworks.com)) that will be used to check hashes and files.

STEP 8 | By default, the ESM Server submits files up to 100MB to WildFire for analysis. To change the maximum file size, enter a value from 1 to 100 (MB). Files that exceed the maximum size are not submitted to WildFire either automatically or manually.

STEP 9 | **Save** your changes.

### Configure a WildFire Rule

WildFire rules determine how Traps detects and responds to malware on your endpoints. You can create or edit WildFire rules on the [WildFire rule management page](#). When you configure a WildFire rule, you can enable any of the following functionality in Traps:

- Notify the user about malware on the endpoint
- Execute the desired action on malware (either block, permit but notify, or permit and silently log the event)
- Apply the same action on malware to grayware
- Submit unknown files to the ESM Server for WildFire analysis
- Use local analysis to determine the verdict for a file
- Quarantine malicious files
- Block unknown files when no WildFire verdict is available
- Block unknown files when the ESM Server is unreachable

By default, a WildFire rule applies to all users. If needed, you can customize different WildFire settings for specific users or different groups of users by creating a WildFire rule for each.

STEP 1 | Verify that the ESM components are configured to communicate with WildFire.

See [Set Up the ESM to Communicate with WildFire](#).

STEP 2 | Configure a new WildFire rule.

1. Select **Policies > Malware > WildFire**.
2. **Add** a new rule or select and **Edit** an existing rule.

STEP 3 | **Activate** the WildFire module to enable Traps to calculate and check hash verdicts against its local cache of hashes.

*To get the most out of WildFire integration, we recommend that you turn on all WildFire functionality.*
Set **WildFire Activation** to **On** and then configure any additional behavior, as needed.

- Enable the ESM Console to **Upload files for WildFire analysis**. When enabled, Traps sends only unknown executable files to the ESM Console, which sends the files to WildFire for analysis.
- Enable Traps to perform **Local Analysis** to determine the likelihood that an unknown executable file is malware.
- Enable Traps to **Quarantine Files** that have a malware verdict (determined by WildFire, administrative policy override, or local analysis).

**STEP 4 |** Configure the **Action**—the behavior of Traps—when Traps identifies malware.

- Select **Inherit** to use the behavior defined by the default policy (Prevention).
- Select **Prevention** to block the malicious executable file.
- Select **Notification** to allow the user to open the executable file, log the issue, and notify the user about the malicious file.
- Select **Learning** to allow the user to open a malicious executable file and silently log the issue without notifying the user.
- To apply the same action as malware to grayware, enable the **Apply action on grayware** setting. Otherwise, if this option is not selected, grayware is considered benign and is not blocked.

**STEP 5 |** Configure the treatment of unknown executables when Traps cannot identify a verdict.

By default Traps permits unknown executable files to open; however, if local analysis is enabled, Traps always returns a verdict for an unknown executable file. Therefore, enabling these options files only applies to agents for which local analysis is not enabled or for agents running versions earlier than Traps 3.4.

- Enable Traps to always **Block unknown files** when the verdict is unknown in the local cache.
- If the ESM is unreachable, Traps issues the file a no-connection verdict. To specifically block files that have this type of verdict, enable the option to **Block unknown files while not connected to the ESM**.

**STEP 6 |** Specify whether Traps will notify the user about the malicious executable file.

From the **User Alert** drop-down, select **On** to notify the user or **Off** to silently log the event.

**STEP 7 | (Optional) Add Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 8 | (Optional) Define the Target Objects** to which to apply the WildFire rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 9 | (Optional) Review the rule name and description.** The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 10 |** Save the WildFire rule.
Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Policies > Malware > WildFire** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **WildFire** page at any time to **Delete** or **Deactivate** the rule.
Manage Hashes for Executable Files

When WildFire integration is enabled, Traps calculates a unique hash using the SHA-256 algorithm for executable files run on an endpoint and checks it against WildFire. The Hash Control page displays the WildFire response for each hash sent to WildFire.

If WildFire has already analyzed an executable file and determined that it is malware, WildFire sends a response that identifies the executable file as Malicious. If WildFire has already analyzed an executable file and determined that it contains no malicious code or behavior, then WildFire sends a response that identifies the executable file as Benign. If WildFire has not previously analyzed the executable file, it responds with a status of Unknown and, if the ESM Server cannot reach WildFire at all, the ESM Server marks the status of the file as No Connection. You can specify the actions associated with malicious, benign, unknown, and no connection verdicts in the WildFire integration settings (see Set Up the ESM to Communicate with WildFire).

- View and Search Hashes
- Export and Import Hashes
- View a WildFire Report
- Override a WildFire Verdict
- Recheck a WildFire Decision
- Report an Incorrect Verdict
- Upload a File to WildFire for Analysis
- Manage Quarantine Settings
- Restore a Quarantined File

View and Search Hashes

The Hash Control page displays a table of all the hashes and their verdicts for executable files reported by the Traps agents in your organization. A search field at the top of the page allows you to filter results by a full or partial string. The search engine queries the hash values and process names and returns any matching results. Searching for a full hash value returns the record for only that unique hash, if found; searching for a process name returns any hash records that match the process name, if found.

Export and Import Hashes

The Hash Control page displays information about the hashes and the verdicts associated with all executable files that users or machines have tried to open on your endpoints. Use the export function from the action menu to back up hash records before migrating or upgrading to a new server or
before deploying hash records to multiple independent servers. You can export hash records on a global or individual basis and save them to an XML file. Importing hash records appends any new hashes to the existing Hash Control table.

If you attempt to edit the XML file in Excel, Excel automatically adds quotes around some values in the file. These quotes do not adhere to the input format expected by the ESM Console. Therefore, if you need to modify the XML file, you must use a text editor to remove the quotes before attempting to import the file.

**STEP 1** | From the ESM Console, select **Policies > Malware > Hash Control**.

**STEP 2** | Do either of the following:

- To back up or export hash records, select the check box next to the record(s) you want to export. From the action menu at the top of the table, select **Export Selected**. The ESM Console saves the selected hash records to an XML file.
- To restore or import new policy rules, select **Import Hashes** from the action menu at the top of the table. Browse to the XML file and then **Upload**.

**View a WildFire Report**

To help aid in hash control decisions, you can view a copy of the official WildFire report for each executable file that WildFire analyzes. The ESM Server caches the report and makes it available on the **Hash Control** page of the ESM Console. Each report contains file information, a behavioral summary about the executable file, and details about network and host activity.

**STEP 1** | From the ESM Console, select **Policies > Malware > Hash Control**.

**STEP 2** | Search for and then select the hash for which you would like to see the report.

**STEP 3** | Click **WildFire Report**. The ESM Console displays the cached report.

**STEP 4** | Review the report and take additional action, as needed:

- **Override a WildFire Verdict**
Override a WildFire Verdict

You can locally override a WildFire verdict to allow or block a file without impacting the official verdict in WildFire. This is useful when you need to create an exception for a specific file in only specific circumstances or endpoints without altering the global security policy. After overriding the verdict, the ESM Console displays any change in the WildFire verdict on the Hash Control page. The override remains in place until you remove it, at which time it reverts to the last known verdict on the server.

For example, consider a case where WildFire returns a verdict on a specific hash and indicates that the file is unknown. If your security policy is configured to block all unknown files and you believe the file to be benign, you can override the policy to allow the specific file to execute without altering the global policy. Later, if WildFire returns a new verdict indicating that the file was analyzed and determined to be malicious, you can view the verdict change on the Hash Control page. In that case, you can remove the override and allow the security policy to block the malicious file.

**STEP 1** | From the ESM Console, select Policies > Malware > Hash Control.

**STEP 2** | To view the WildFire verdict for a specific hash, do either of the following:

- Use the search at the top of the page to search for a hash value or process name.
- Use the paging controls on the top right of each page to view different portions of the table.

**STEP 3** | To review the endpoints on which a user has tried to open the executable file, select Agent List (available only when there are five or more instances of a process hash).

**STEP 4** | Review the WildFire report for the executable file to validate your decision to override the verdict. See View a WildFire Report.

**STEP 5** | Select the hash record and then click Treat as Benign to allow the executable file to run or click Treat as Malware to block execution of the file. This override does not affect the official WildFire verdict but it does change the verdict in the local security policy for your organization. If you suspect a WildFire verdict is incorrect, please consider reporting the issue to Palo Alto Networks. See Report an Incorrect Verdict.

**STEP 6** | On a regular basis, review any mismatches between the official WildFire verdict and your local policy action.

**STEP 7** | When the override is no longer needed, remove it. From the action menu, select Revert to WildFire Verdict. The ESM Console reverts to the verdict last known by the ESM Server.

Recheck a WildFire Decision

If you suspect that WildFire has changed the verdict of a file, you can force the ESM Server to query WildFire for the verdict. If the WildFire response indicates a change to the verdict, the ESM Server updates the verdict in its local server cache. Then, at the next heartbeat communication with Traps agents, the ESM Server communicates the verdict to endpoints on which a user has tried to open the executable file.

**STEP 1** | From the ESM Console, select Policies > Malware > Hash Control.

**STEP 2** | To view the WildFire verdict for a specific hash, do either of the following:
- Use the search at the top of the page to search for a hash value or process name.
- Use the paging controls on the top right of each page to view different portions of the table.

**STEP 3** | Select the hash record to view additional details about the process hash and then click **Recheck**. To recheck multiple records at the same time, select the check box for each hash record, and then select **Recheck with WildFire** from the action menu. These actions initiate an immediate query to WildFire.

**Report an Incorrect Verdict**

When you want WildFire to reanalyze a file and change its official verdict, you can use the **Report Incorrect Verdict** feature from the **Policies > Malware > Hash Control** page on the ESM Console. This action flags a sample for further analysis by Palo Alto Networks.

When reporting an incorrect file verdict, you can provide your email address and additional information about why you believe the verdict is incorrect. If you choose to provide your email address, you will receive an email notification containing the results of the analysis. If WildFire changes the verdict, the ESM Console also displays the updated verdict on the **Hash Control** page.

**STEP 1** | Locate the verdict and report it to WildFire.

1. From the ESM Console, select **Policies > Malware > Hash Control**.
2. In the search field, enter the full or partial hash value or process name and then click the search icon to filter the list of hashes.
3. Select the row for the hash to expand the hash details and then click **Report as Incorrect**.

**STEP 2** | Fill out the report with details that indicate why the verdict is incorrect.

1. Review the sample information and verify the verdict that you are reporting.
2. (Optional) Enter an email address to receive an email notification after Palo Alto Networks completes the additional analysis.
3. (Optional but recommended) Enter any details that may help us to better understand why you disagree with the verdict.
4. Click **Submit**.

**Upload a File to WildFire for Analysis**

Before the integration of the Traps solution, WildFire typically only analyzed an executable file if it was sent through or uploaded from the firewall or if it was submitted using the WildFire portal. This meant that some executable files, while common, may not have been analyzed because it was not common to submit them using the traditional methods. To reduce the number of executable files that are unknown by the ESM Server and by WildFire, you can manually or automatically send unknown executable files to WildFire for immediate analysis. To automatically send unknown files to WildFire, see **Set Up the ESM to Communicate with WildFire**.

If the option to automatically send unknown files is disabled, you can instead manually upload a file on a case-by-case basis. When a user opens an unknown executable file, Traps uploads the file to the forensic folder (so long as the file does not exceed the configured maximum size in **Step 8 when you Set Up the ESM to Communicate with WildFire**). Then, when you initiate a manual upload of the file, the ESM Server sends the file from the forensic folder to WildFire.

After WildFire completes its analysis and returns the verdict and report, the ESM Server sends the changed verdict to all Traps agents and enforces the policy.
As more agents enable automatic forwarding of unknown files or submit them manually, the total number of unknown files is expected to decrease dramatically for all users.

**STEP 1** | From the ESM Console, select **Policies > Malware > Hash Control**.

**STEP 2** | To view the WildFire verdict for a specific hash, do one of the following:
- Use the search at the top of the page to search for a hash value or process name.
- Use the paging controls on the top right of each page to view different portions of the table.
- Filter the table entries by clicking the filter icon to the right of a column to specify up to two sets of criteria by which to filter the results. For example, filter the Verdict column for unknown files.

**STEP 3** | Select the row to view additional details about the process hash and then **Upload** the file to WildFire.

### Manage Quarantine Settings

To prevent malware from causing harm to data or systems, you can enable Traps to quarantine files.

Before Traps can begin quarantining files:
- Enable Traps to quarantine files in a WildFire rule. See **Configure a WildFire Rule**.
- Adjust the storage quota for event logs (see **Define Event Logging Preferences**). Traps stores quarantined files in the same location as the logs. When the storage folder reaches the size quota, Traps makes room for new logs by deleting the oldest logs first.

### Restore a Quarantined File

When malware is launched on the endpoint, and Traps is enabled to quarantine files, Traps take immediate action to quarantine the malicious executable file. To evaluate whether an executable file is considered malicious, Traps uses information from the following sources:
- WildFire threat intelligence
- Local analysis
- Administrative hash control policy (a verdict override configured in the ESM server cache)

When any of these sources identify malware, Traps moves the malware from the local folder or removable hard-drive to a local quarantine folder (%PROGRAMDATA%\Cyvera\Quarantine). If user alerts are enabled, Traps also notifies the user about the quarantined file.

If after using available threat intelligence—such as from WildFire or AutoFocus—you believe the quarantined file is not malware and is benign, you can update your hash control policy and then restore the executable file to its original location (either on the endpoint, or on a removal drive).

*When the same malware file (same filename and hash) runs from multiple locations, the Hash Control page only displays information about the last instance. As a result, if you choose to restore a file, you can only restore the last instance.*

Each time you restore an executable file, the ESM Console sends a one-time action rule to the agent to restore the file. You can also use **Cytool** to view and restore quarantined files (see **Restore a Quarantined File Using Cytool**). To view the quarantine and restoration status, view the logs or configure the ESM to send logs to an external logging server.

**STEP 1** | Review quarantined files.
Each time Traps quarantines a file, the ESM Console logs a quarantine event. The ESM Console also updates the hash control record to indicate the quarantine status and number of endpoints on which the file was quarantined.

1. Log in to the ESM Console and select Policies > Malware > Hash Control.
2. From the action menu ≡ -, select Restore Candidates. The ESM Console filters the results to display only quarantined files. You can also filter the Quarantined column by the value Yes. (To return to the unfiltered review of hashes and refresh the results, remove the filter at the top of the table or select Hash Control from navigation menu on the left.)
3. To view additional information about the executable file, select the row for a hash record. The row expands to display additional fields.
4. To view the endpoints on which the executable file was quarantined, click Agent List. The Quarantined Status column indicates whether quarantine was successful on each endpoint. Click the x to close the agent list.

**STEP 2 |** Configure an administrative hash control policy for the executable file. Each time a user attempts to run an executable file, Traps evaluates whether the file is malware and whether to quarantine the file. If you choose to restore an executable file but do not change the Hash Control policy, the next time a user attempts to run the file, Traps blocks and then quarantines the file again. Therefore, to prevent Traps from continuing to block and quarantine a file, you must configure an administrative hash control policy to Treat as Benign.

In the additional details view of the hash record, select Treat as Benign. You can also select the checkbox next to the row or rows and select Treat as Benign from the action menu ≡ -. This changes the verdict in the server cache from Malware to Benign.

**STEP 3 |** Restore a quarantined file.

In the expanded details view for the hash record, click Restore and confirm the action to restore the file on one or more endpoints. You can also select the checkbox next to the row or rows and select Restore from the action menu ≡ -. When Traps receives the request at its next heartbeat communication with the ESM Server, it attempts to restore the file to its original location on each endpoint.

*The Restore button is disabled (grayed out) if the file is not quarantined.*

**STEP 4 |** (Optional) View logs for restored files on the agent.

You can also forward reports for these events to an external logging server or to an email address. See Reports and Logging.

Select Monitor > Agent > Logs. Filter the Report Type by any of the following events:

- **File Restore Succeeded**—Traps successfully restored an executable file to its original location on an endpoint.
- **File Restore Failed**—Traps failed to restore an executable file to its original location on an endpoint.
Manage Restrictions on Executable Files

Restriction rules enable you to define limitations on where and how the Traps agent handles executable files on the endpoints in your network.

- Restriction Rules
- Wildcards and Variables in Restriction Rules
- Add a New Restriction Rule
- Manage Global Whitelists
- Block Execution from Local Folders
- Block Execution from Network Folders
- Define External Media Restrictions and Exemptions
- Define Child Process Restrictions
- Define Java Restrictions and Exemptions
- Define Unsigned Executable File Restrictions and Exemptions

Restriction Rules

A restriction rule limits the surface of an attack by defining where and how your users can run executable files. The following table displays the different types of restrictions you can configure:

<table>
<thead>
<tr>
<th>Restriction Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running executable files from certain folders</td>
<td>Many attack scenarios are based on writing malicious executable files to certain folders and then running them. It is advisable to restrict access to local temp and download folders on the endpoints and to network folders. To make an exception to this general restriction, you can add specific folders to a whitelist. For more information, see Manage Global Whitelists, Block Execution from Local Folders, and Block Execution from Network Folders.</td>
</tr>
<tr>
<td>Running executable files from external media</td>
<td>Malicious code can gain access to endpoints via external media such as removable drives and optical drives. To protect against this, you can define restrictions that control the executable files, if any, that users can launch from external drives attached to the endpoints in your network. For more information, see Define External Media Restrictions and Exemptions.</td>
</tr>
<tr>
<td>Processes spawning child processes</td>
<td>Malicious code can activate by causing a legitimate process to spawn malicious child processes. You can block the malicious code by defining an appropriate restriction rule. For more information, see Define Child Process Restrictions.</td>
</tr>
<tr>
<td>Java processes run from browsers</td>
<td>A common entry point for malicious code is through Java processes that are imported from a remote host and launched through Internet browsers. To protect against these exploits, you need to prevent untrusted Java applets from executing objects using browsers while whitelisting specific trusted processes so they can run on endpoints as needed. You can selectively choose which actions are permitted (read, write, or execute) based on process file types, locations, and registry paths. For more information, see Define Java Restrictions and Exemptions.</td>
</tr>
</tbody>
</table>
Restriction Rules | Description
---|---
**Running unsigned processes** | A signed process has a digital authentication signature to prove that the signature comes from a trusted source. Best practice dictates that all legitimate applications be signed but this practice is not always followed. Restrictions on unsigned processes prevent all unsigned processes from running on your endpoints except those you explicitly whitelist. You can also define a postponement period, which prevents unsigned processes from running for a certain number of minutes after they are initially written to the disk on the endpoint. Because an attack can involve writing a malicious executable file to the disk and running it immediately, using a postponement period and restricting unsigned processes is effective at preventing malware attacks. For more information, see Define Unsigned Executable File Restrictions and Exemptions.

For each restriction, you specify the target object(s), condition(s), restriction type, and action(s) for managing executable files. A target object can be any user, group, organizational unit, or computer that appears in Active Directory or any endpoint on which the Traps agent is installed. The Endpoint Security Manager identifies endpoints using the messages the Traps agent sends to the server. A condition can refer to a specific file, a specific version or range of versions for a file, or a registry path that must exist on the endpoint.

When a user attempts to open an executable file, the Traps agent evaluates which, if any, restriction rules it needs to apply to the file and then performs the actions associated with those applied rules. The actions determine whether the Traps agent will prevent the file from executing and whether the agent will notify the user when a restriction rule is triggered.

You can create or edit restriction rules on the Restrictions summary and management page (Policies > Malware > Restrictions). Selecting a rule displays further information about the rule and other actions you can take for that rule (Delete, Activate/Deactivate, or Edit). For more information, see Manage Restrictions on Executable Files.

**Wildcards and Variables in Restriction Rules**

When configuring a restriction rule, such as to configure local or network folder behavior, you add one or more files or folders to a whitelist or blacklist. The path can be a full path or a partial path that contains wildcards (“*” or “?”) and/or environment variables.

- Wildcards in Restriction Rules
- Environment Variables in Restriction Rules
- Example: Using Wildcards and Variables in Restriction Rules

**Wildcards in Restriction Rules**

The following table displays the wildcards that you can use in restriction rules to match a filename (regardless of location), a file located within a specific folder or folder path, or any file within a specific folder or folder path.

<table>
<thead>
<tr>
<th>Value</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Matches a single character. For example, *wor?.exe matches *Word.exe and *Worm.exe.</td>
</tr>
</tbody>
</table>
Environment Variables in Restriction Rules

In addition to wildcards, restriction rules also support native environment variables, including user- and system-wide variables. Restriction rules also support the use of multiple environment variables as long as the environment variable does not expand to another environment variable. You can use many environment variables that are supported by the Windows OS but some environment variables, including this specific set of variables, are not supported:

- `%USERNAME%` environment variable
- Environment variables that are private
- Recursive environment variables which include other environment variables in their definition (for example, `%MySystemDrive%` with a definition of `%SystemDrive%`)

The following topics describe supported environment variables in Windows and examples of the target values.

- Environment Variable Support for Windows Vista and Later Releases
- Environment Variable Support for Windows XP

Environment Variable Support for Windows Vista and Later Releases

The following table displays environment variables and target values supported on endpoints running Windows Vista and later releases.

> The `%CommonProgramFiles(x86)%` and `%ProgramFiles%` environment variables expand to the native value of the machine. On 64-bit machines, the environment variable expands to the 64-bit value even when operating on behalf of a 32-bit process. On 32-bit machines, the environment variables expands to the file path provided by the application.

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ALLUSERSPROFILE%</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>%AppData%</td>
<td>C:\Users&lt;username&gt;\AppData\Roaming</td>
</tr>
<tr>
<td>%LocalAppData%</td>
<td>C:\Users&lt;username&gt;\AppData\Local</td>
</tr>
<tr>
<td>%CommonProgramFiles%</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>%CommonProgramFiles(x86)% (64-bit only)</td>
<td>C:\Program Files (x86)\Common Files</td>
</tr>
<tr>
<td>%CommonProgramW6432% (64-bit only)</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>%ProgramFiles%</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>%ProgramFiles(x86)% (64-bit only)</td>
<td>C:\Program Files (x86)</td>
</tr>
<tr>
<td>%ProgramW6432% (64-bit only)</td>
<td>C:\Program Files (x86)</td>
</tr>
</tbody>
</table>
## Environment Variable Support for Windows XP

The following table displays examples of environment variables and target values supported on endpoints running Windows XP.

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ALLUSERSPROFILE%</td>
<td>C:\Documents and Settings\All Users</td>
</tr>
<tr>
<td>%AppData%</td>
<td>C:\Documents and Settings&lt;username&gt;\Application Data</td>
</tr>
<tr>
<td>%LocalAppData%</td>
<td>C:\Documents and Settings&lt;username&gt;\Local Settings</td>
</tr>
<tr>
<td>%CommonProgramFiles%</td>
<td>C:\Program Files\Common Files</td>
</tr>
</tbody>
</table>
Environment Variable | Example Value
--- | ---
%ProgramFiles% | C:\Program Files
%SystemDrive% | C:
%SystemRoot% | C:\Windows
%TEMP% and %TMP% | C:\Documents and Settings\<username>\Local Settings\Temp
%USERPROFILE% | C:\Documents and Settings\<username>
%windir% | C:\Windows
%COMPUTERNAME% | <computername>
%ComSpec% | %SystemRoot%\system32\cmd.exe
%FP_NO_HOST_NAME% | NO
%NUMBER_OF_PROCESSORS% | 1
%OS% | Windows_NT
(PATH% | %SystemRoot%\system32;%SystemRoot%
%PATHEXT% | .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
%PROCESSOR_ARCHITECTURE% | x86
%PROCESSOR_IDENTIFIER% | x86 Family 6 Model 58 Stepping 9, GenuineIntel
%PROCESSOR_LEVEL% | 6
%PROCESSOR_REVISION% | 3a09

Example: Using Wildcards and Variables in Restriction Rules

The following table displays examples of using wildcards and variables to specify a filename (regardless of location), a file located within a specific folder or folder path, or any file within a specific folder or folder path.

<table>
<thead>
<tr>
<th>Example</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\temp\a.exe</td>
<td>Matches only the a.exe file and only if launched from the C:\temp folder</td>
</tr>
<tr>
<td>%TEMP%\a.exe</td>
<td>Matches only the a.exe file and only if launched from the C:\Users &lt;username&gt;\AppData\Local\Temp folder on Windows Vista and</td>
</tr>
<tr>
<td>Example</td>
<td>Result</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>later machines or C:\Documents and Settings&lt;username&gt; \Local Settings\Temp on Windows XP machines</td>
<td></td>
</tr>
<tr>
<td>C:\temp*</td>
<td>Matches any file launched from the C:\temp folder or from any folder or subfolder in a filepath that begins with C:\temp (for example, C:\temp\folder\a.exe, C:\temp1\a.scr, and C:\temporary\folder \b.exe)</td>
</tr>
<tr>
<td>C:\temp*</td>
<td>Matches any file launched from the C:\temp folder or subfolder (for example: C:\temp\a.scr and C:\temp\temp2\b.exe)</td>
</tr>
<tr>
<td>C:\temp\a?.exe</td>
<td>Matches any file beginning with a and followed by a second character launched from the C:\temp folder (for example: C:\temp\a1.exe and C:\temp\az.exe)</td>
</tr>
<tr>
<td>C:\temp*.exe</td>
<td>Matches any executable file with an .exe file extension, a filename that begins with temp, and that is launched from the C:\ drive (for example, C:\temp1.exe and C:\temporary.exe) and matches any executable file with an .exe file extension that is launched from any folder or subfolder in a filepath that begins with C:\temp (for example, C:\temp\folder\a.exe, C:\temp1\b.exe, and C:\temporary\folder \c.exe)</td>
</tr>
<tr>
<td>C:\temp*.exe</td>
<td>Matches any executable file with an .exe file extension that is launched from the C:\temp\ folder (or equivalent %SystemDrive%\temp\ folder) or from any folder or subfolder in a filepath that begins with C:\temp</td>
</tr>
<tr>
<td>%SystemDrive%\temp *.exe</td>
<td></td>
</tr>
<tr>
<td>*\a.exe</td>
<td>Matches only the a.exe file regardless from which location it is launched</td>
</tr>
<tr>
<td>%SystemDrive%\ %MyVar%</td>
<td>When %MyVar% is equal to a filename, for example myfile.exe, this matches that filename when launched from the %SystemDrive% folder (in most cases C:)</td>
</tr>
<tr>
<td>a.exe</td>
<td>(Java or unsigned executable restriction rules only) Matches only the a.exe file regardless from which location it is launched</td>
</tr>
<tr>
<td>Java and unsigned executable restriction rules require you to include the .exe at the end of the filename.</td>
<td></td>
</tr>
<tr>
<td>C:\temp</td>
<td>Does not match any executable files because the path is not a full path (partial paths must contain at least one wildcard to be useful)</td>
</tr>
</tbody>
</table>

### Add a New Restriction Rule

Create a new restriction rule to define limitations on where and how executable files run on endpoints.

**STEP 1 |** Configure a new restriction rule.

Select Policies > Malware > Restrictions and Add a new rule.
STEP 2 | Select the type of restriction rule you are adding.

Select one of the following options and then configure settings according to the type of restriction you are adding to your security policy:

- **Local Folder Behavior**—Restrict access to local folders on the endpoints. For more information, see Block Execution from Local Folders.
- **Network Folder Behavior**—Restrict access to network folders. For more information, see Block Execution from Network Folders.
- **External Media**—For more information, see Define External Media Restrictions and Exemptions.
- **Child Processes**—Block malicious child processes spawned from legitimate processes. For more information, see Define Child Process Restrictions.
- **Java**—Prevent untrusted Java applets from executing objects using browsers and add specific trusted processes to whitelists so they can run on endpoints as needed. For more information, see Define Java Restrictions and Exemptions.
- **Unsigned Executables**—Prevent all unsigned processes from running on your endpoints except those you explicitly whitelist. For more information, see Define Unsigned Executable File Restrictions and Exemptions.

STEP 3 | (Optional) Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the **Target Objects** to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

STEP 6 | Save the restrictions rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Policies > Malware > Restrictions** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Restrictions** page at any time to **Delete** or **Deactivate** the rule.

**Manage Global Whitelists**

To allow executable files to run from local folders and external media and allow child processes initiated from parent processes in a specific folder, you can configure a global whitelist. Similar to the existing whitelist functionality for Java processes, unsigned executable files, and Thread Injection, you can specify
full paths and path variables and can also use wildcards for pattern matching (% to match similar terms and * to match any characters).

Items in the whitelist section also take precedence over any blacklisted items and are evaluated first in the security policy.

STEP 1 | **Select Policies > Malware > Restriction Settings.**

STEP 2 | To specify whether Traps blocks an executable file that it is opened from a location not included in the whitelist or that is younger than the block period, configure the **Action** as one of the following:

- **Notification**—Do not block access to executable files and processes but log when files that are opened from locations not included in the whitelist and report those events to the ESM.
  
  or

- **Prevention**—Block executable files and processes.

STEP 3 | To specify whether Traps should notify the user when an executable file is opened from a location not included in the whitelist, configure the **User Alert** as one of the following:

- **On**—Notify the user.
  
  or

- **Off**—Do not notify the user.

STEP 4 | Click the add folder icon next to the whitelist area for Local Folder, Child Process, or Media Control and enter the full path or partial path. For example, C:\Windows\filename.exe.

  *Whitelists also support wildcards (see Wildcards and Variables in Restriction Rules) and environmental variables, such as $windir$.*

STEP 5 | To specify a block period for unsigned files, select the **Allow signed executables and block unsigned executables created** option. Then configure the block period (in minutes) for which
Traps should block an unsigned executable file that is not defined in the whitelist, or select **Any time** to configure Traps to always block executable files that are unsigned.

*Traps permits all signed executables to run regardless of block period.*

*You cannot specify a block period for unsigned executable files that execute on external media.*

**STEP 6** | Click **Commit** to save your changes.

### Block Execution from Local Folders

Many attack scenarios are based on writing malicious executable files in common local folders, such as temp and download, and then running those executable files. By default, Traps allows benign executable files to run from any local folder. To restrict a specific executable file or execution from running from a local folder commonly used in attack scenarios, add the file or folder to a blacklist. When a user attempts to open a file that is blacklisted or located in a blacklisted folder, Traps blocks the attempt and reports the security event to the ESM Server.

To grant an exception on the general restriction you can also add a local folder to a whitelist (see **Manage Global Whitelists**). The global whitelist takes precedence over the blacklist and enables executable files in specific locations to always run.

**STEP 1** | **Configure a new restrictions rule.**

Select **Policies > Malware > Restrictions** and **Add** a new rule.

**STEP 2** | **Block an executable file or files run from a local folder.**

1. **Select Local Folder Behavior.**
2. **Select the option to Restrict file execution from the locations.**
3. Click the add folder icon 🔗, and **Add** the executable file or folder path to the Blacklist section.

*To blacklist a folder, you must terminate the path with a wildcard. For example, C:\temp\* matches any file launched from the C:\temp\ folder or subfolder.*

For additional syntax examples, see **Wildcards and Variables in Restriction Rules**.

4. Repeat the previous step to add multiple paths as needed.

**STEP 3** | **(Optional) Add Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 4** | **(Optional) Define the Target Objects** to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users, Computers, Groups, Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.
STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the restrictions rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Policies > Malware > Restrictions page and then click Activate.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Restrictions page at any time to Delete or Deactivate the rule.

Block Execution from Network Folders

To prevent attack scenarios that are based on writing malicious executable files to remote folders, you can create a restriction rule that defines **Network Folder Behavior**. When enabled, Traps blocks all executable files that run from network locations. To allow executables to run from trusted networked folders, you must add the file or folder path to a whitelist. When a user attempts to open an executable file from a network folder that is not specified in the whitelist, Traps blocks the attempt and reports the security event to the ESM Server.

STEP 1 | Configure a new restrictions rule.

Select Policies > Malware > Restrictions and Add a new rule.

STEP 2 | Enable Traps to block executable files run from network folders.

1. Select Network Folder Behavior.
2. Select the option to Restrict file execution from all network folders.
3. (Optional) To permit executable files to run from trusted network folders, click the add folder icon, and Add the file or folder path to the Whitelist section.

   To whitelist a folder, you must terminate the path with a wildcard. For example, \networkpath\temp\* matches any file launched from the \networkpath\temp folder or subfolder).

   For additional syntax examples, see Wildcards and Variables in Restriction Rules.
4. Repeat the previous step to add multiple paths as needed.

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the Target Objects to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas.
The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5 | (Optional)** Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

**STEP 6 |** Save the restrictions rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Policies > Malware > Restrictions page and then click Activate.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Restrictions page at any time to Delete or Deactivate the rule.

**Define External Media Restrictions and Exemptions**

Malicious code can gain access to endpoints through external media, such as removable drives and optical drives. To protect against this type of attack, you can define restriction rules that prevent executable files from running on external drives that are attached to your endpoints. Defining a restriction on external media protects against any attempt to launch an executable file from an external drive.

**STEP 1 |** Configure a new restrictions rule.

Select Policies > Malware > Restrictions and Add a new rule.

**STEP 2 |** Define the restriction behavior for external media. By default, running non-malicious and unknown applications from removable and optical drives is allowed.

1. Select External Media.
2. Select the check box for the type of external media from which you want to prevent applications from running.
   - Removable Drives
   - Optical Drives

**STEP 3 | (Optional)** Add Conditions to the Rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

**STEP 4 | (Optional)** Define the Target Objects to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.
STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the restrictions rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Policies > Malware > Restrictions page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Restrictions page at any time to **Delete** or **Deactivate** the rule.

Define Child Process Restrictions

In an attempt to control an endpoint, an attacker can cause a legitimate process to spawn malicious child processes. Define a restriction rule to prevent child processes from launching from one or more processes.

STEP 1 | Configure a new restrictions rule.

Select Policies > Malware > Restrictions and **Add** a new rule.

STEP 2 | Define the restriction behavior for child processes. By default, child processes spawned from a process are allowed.

2. In the Select Processes search field, enter and then select the name of the process. As you type, the ESM Console displays any processes that match your search term.

   To modify the processes list, see Manage Processes.

3. Repeat steps 2.b to add additional process names, as needed.

STEP 3 | (Optional) Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the **Target Objects** to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.
To override the autogenerated name, select the Name tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6 | Save the restrictions rule.**

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Policies > Malware > Restrictions page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Restrictions page at any time to **Delete** or **Deactivate** the rule.

### Define Java Restrictions and Exemptions

A common entry point for malicious code is through Java processes that are imported from a remote host and run in Internet browsers. To protect against these exploits, you can configure Traps to prevent a Java applet from executing objects from within web browsers and whitelist only trusted processes so they can execute as needed. Use the whitelist option to selectively choose which file types, locations, and registry paths for which these processes are allowed to read and write.

**STEP 1 | Configure a new restrictions rule.**

Select **Policies > Malware > Restrictions** and **Add** a new rule.

**STEP 2 | Define the restrictions on Java processes.**

*By default, Java process restrictions are disabled. Enabling the Java restriction rule allows you to place restrictions on the Java processes but does not enable or disable any of the EPM rules.*

1. Select **Java**.
2. Select **Java Activation** drop-down, select **On** to enable the rule or **Off** to disable the rule.

*Any additional settings are grayed out if Java is disabled.*

3. Configure the **Action** to take when a Java process attempts to call a child process, modify registry settings, or modify system files from a web browser:
   - **Inherit**—Inherit the behavior from the default policy.
   - **Prevention**—Terminate the Java process.
   - **Notification**—Log the issue and allow the Java process to continue.

4. Configure the **User Alert** behavior when a Java process attempts to call a child process, modify registry settings, or modify system files from a web browser:
   - **Inherit**—Inherit the behavior from the default policy.
   - **On**—Notify the user.
   - **Off**—Do not notify the user.

5. In the Java Whitelisted Processes section, click the add processes button ✷ to specify the Java processes that will be allowed to run from web browsers (for example **AcroRd32.exe**). Repeat this step to add additional processes.

6. To specify whether a Java process can modify registry settings, select **Enabled** from the Registry Modifications drop-down and then configure the registry permissions:
1. For each registry path, set each permission (Read, Write, and Delete) to Allow, Block, or Inherit (default).
2. Click the add registry paths button to add additional registry paths as needed.
7. To specify whether a Java process can read or write to a file, select Enabled from the File System Modifications drop-down and then configure the file permissions:
   1. For each new file pattern, set each permission (read and write) to Allow, Block, or Inherit (default).
   2. Click the add file pattern button to add a new file pattern.
8. From the Browsers list, select the web browsers on which to enforce Java protection.

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the Target Objects to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the restrictions rule.

Do either of the following:

- Save the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Policies > Malware > Restrictions page and then click Activate.
- Apply the rule to activate it immediately.

After saving or applying a rule, you can return to the Restrictions page at any time to Delete or Deactivate the rule.

Define Unsigned Executable File Restrictions and Exemptions

A signed process has a digital signature to prove that the signature comes from a trusted source. Best practice dictates that all legitimate applications are signed. Restrictions on unsigned processes prevent all unsigned processes from running except those you explicitly allow. You can also define a postponement period, which prevents unsigned processes from launching for a certain number of minutes after they are initially written to the disk on the endpoint. Because an attack can involve writing a malicious executable file to the disk and running it immediately, using a postponement period and restricting unsigned processes is effective in preventing malware attacks.

STEP 1 | Configure a new restrictions rule.

Select Policies > Malware > Restrictions and Add a new rule.
STEP 2 | Define the restrictions on unsigned executable files.

1. Select **Unsigned Executables**.
2. Configure the **Action** to take when a user opens an unsigned executable:
   - **Inherit**—Inherit the behavior from the default policy.
   - **Prevention**—Block the process.
   - **Notification**—Log the issue and allow the process to continue.
3. Configure the **User Alert** behavior when a user opens an unsigned executable.
   - **Inherit**—Inherit the behavior from the default policy.
   - **On**—Notify the user.
   - **Off**—Do not notify the user.
4. Specify the **Blacklist Period** (in minutes) to prevent unsigned processes from running for a specified amount of time after the executable file is initially written to the disk on the endpoint.
5. To allow a process to run immediately without waiting for the blacklist period to expire, click the add processes button and add the process as one of the **Whitelisted Processes**.
6. To allow all processes under a certain folder to run immediately without waiting for the blacklist period to expire, click the add folders button and add the folder to the **Whitelisted Paths**.

STEP 3 | *(Optional)* Add **Conditions** to the Rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | *(Optional)* Define the **Target Objects** to which to apply the restriction rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | *(Optional)* Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the restrictions rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Policies > Malware > Restrictions** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Restrictions** page at any time to **Delete** or **Deactivate** the rule.
Manage Malware Protection Rules

Malware protection rules enable you to restrict malware-related behavior. When enabled, these modules use a whitelist model that allows process injection for only those processes specified in the policy. The default malware prevention policies that come preconfigured with the ESM software grant exceptions to common legitimate processes that must inject into other processes or modules.

When new malware protection rules are added to the security policy, the Traps rules mechanism merges all configured rules into an effective policy that is evaluated for each endpoint. In the case of a potential conflict between two or more rules, there are a set of considerations, such as modification date, that determine which rule takes effect. For example, if one rule was created or edited more recently than another, that rule with the later date takes precedence over the rule with a previous date or timestamp. As a result, any new malware protection rules override the default policy, which can cause your policy to be ineffective or cause endpoints to be unstable. Additionally, user-defined whitelists are not merged between different rules and are evaluated only if the associated rule takes precedence.

⚠️ Use caution when configuring new malware prevention policy rules to avoid overriding the default policy and causing instability in your network.

For additional questions about configuring malware protection rules, contact Support team or your Sales Engineer.

To avoid accidentally overriding the default policy, we recommend you configure new rules only on processes that are not covered by the default policy. When configuring a new rule, you can enable the malware module protection for the parent process and use the default policy settings or you can customize the rule settings for your organization. To make changes to the security policy for processes that are already protected, we recommend you use the following workflows when importing or changing the default policies as needed to meet the requirements of your security policy:

- Malware Protection Rules
- Configure Thread Injection Protection
- Manage the Thread Injection Whitelist
- Configure Suspend Guard Protection
- Manage the Suspend Guard Whitelist

Malware Protection Rules

A malware protection rule prevents the execution of malware, often disguised as or embedded in non-malicious files, by using malware modules to target process behaviors that are commonly triggered by malware.

Unlike the exploit protection rules which are opt-in (you enable the modules for the specific processes that you want to protect), the malware protection rules are opt-out (you enable the modules to protect all processes and then specify the processes that are exempt; those processes that are permitted to perform the defined behavior that is disallowed by the malware protection policy).

You can activate malware protection modules in all processes or enable protection of one or more protected processes in your organization.

To allow legitimate processes to execute, you can whitelist parent processes that inject into other processes. Additional whitelist options are available in ninja mode; these advanced whitelist settings allow Palo Alto Networks Support and Sales Engineers to configure additional fine-grained settings for each malware module.

The following table describes the malware protection modules:
### Malware Protection Rules

<table>
<thead>
<tr>
<th>Malware Protection Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspend Guard</td>
<td>Protects against a common malware technique where the attacker creates processes in a suspended state and injects and runs code before the process even starts. You can enable Suspend Guard on a source process mode and can configure the user notification. Optionally, you can also whitelist function modules that can call child processes. For more information, see Configure Suspend Guard Protection.</td>
</tr>
<tr>
<td>Thread Injection</td>
<td>Malicious code can also gain entry by creating remote threads and processes. You can enable Thread Injection to stop remote thread and process creation and specify the limitation on either the source or destination process or thread. Then you can whitelist specific folders to make exceptions to the general restriction rule. For more information, see Configure Thread Injection Protection.</td>
</tr>
</tbody>
</table>

### Configure Thread Injection Protection

A process can comprise one or more threads that execute any part of the process code. Some attack scenarios are based on injecting malicious code into a target process to create remote threads, maintain persistence, and control the infected system.

The default policy contains rules intended to prevent malicious remote thread creation and permits legitimate processes that must inject threads into other processes.

*Use caution when configuring new Thread Injection rules to avoid overriding the default policy and causing instability in your network.*

For additional questions on configuring malware protection rules, contact the Support team or your Systems Engineer.

If the process is not already protected by the default security policy, you can create a new rule that enables Thread Injection protection for a process using the default Thread Injection settings or you can configure the settings as needed for your security policy. Settings include the process name, Activation (On or Off), Action (Prevention or Notification), User Alert (On or Off), and whitelist target processes to which the source process can inject.

If the process is already protected by the default security policy, we recommend you import the default Thread Injection as a new rule and making changes to meet the requirements of your organization. This way, when the policy is activated, it overrides the default policy but still contains the default configuration settings in addition to any changes you made.

**STEP 1 | Configure a Thread Injection rule.**

1. Perform one of the following actions:
   - Add a new rule.
   - Select and Edit an existing rule.
   - Review the default policy rules (select Show Default Rules from the action menu at the top of the table), select a rule, and then Clone it.

2. Select Thread Injection.

**STEP 2 | (Optional) Define the Thread Injection settings.**
To use the settings defined by the default policy, enable the module and then skip to 5.

Alternatively, you can override the defaults to customize the Thread Injection settings as needed for your organization.

1. From the **Activation** drop-down, select **On** to enable the rule or **Off** to disable the rule.

   *Any additional settings are ignored if the malware protection module is disabled.*

2. Configure the **Action** to take when a source process attempts to inject into another process:
   - **Inherit**—Inherit the behavior from the default policy.
   - **Prevention**—Terminate the process.
   - **Notification**—Log the issue and allow the process to inject into another process.

3. Configure the **User Alert** behavior when the source process attempts to inject into another process.
   - **Inherit**—Inherit the behavior from the default policy.
   - **On**—Notify the user when a process tries to inject into another.
   - **Off**—Do not notify the user when a process tries to inject into another.

**STEP 3** | *(New rules only)* Enable Thread Injection protection for a single process or for all processes.

To configure Thread Injection protection for a parent process, select the option to **Select a process** and enter the process name in the field provided. Otherwise, keep the default setting to apply Thread Injection protection to **All Processes**.

**STEP 4** | *(Optional)* Whitelist a target process.

*To avoid overriding the whitelist in the default malware protection policy, we highly recommend that you do not change the Whitelist Actions and, instead, keep the default Merge setting.*

1. Click the ninja mode icon and enter the administrative password.
2. Add one or more processes to the list.

**STEP 5** | *(Optional)* Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 6** | *(Optional)* Define the **Target Objects** to which to apply the malware protection rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 7** | *(Optional)* Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 8** | Save the malware protection rule.
Do either of the following:

- **Save** the rule. This option is only available for inactive, cloned, or new rules. To activate the rule later, select the rule from the **Policies > Malware > Protection Modules** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Policies > Malware > Protection Modules** page at any time to **Delete** or **Deactivate** the rule.

### Manage the Thread Injection Whitelist

If a legitimate process must inject into a specific target process, you can use this workflow to add the target process to a thread injection whitelist.

**STEP 1** | Use the filter to locate the active Thread Injection rule for a specific process.

*This method of filtering rules only works if the Auto Description feature is turned on during rule creation or if you manually enter the process name into the rule description.*

1. Select **Policies > Malware > Protection Modules**.
2. Select the filter icon for the **Description** column.
3. Set the **Show item** criteria to **Contains** and enter a process name in the field provided.
4. Select **Filter**.

**STEP 2** | Modify a malware protection rule.

Select and then **Edit** the rule. If the rule doesn't exist, create it as described in Configure Thread Injection Protection.

**STEP 3** | Add a target process to a whitelist.

1. Click the ninja mode icon and enter the administrative password.
2. Add target process(es) to the list.

**STEP 4** | Save the malware protection rule.

Do either of the following:

- **Save** the rule. This option is only available for inactive, cloned, or new rules. To activate the rule later, select the rule from the **Policies > Malware > Protection Modules** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Policies > Malware > Protection Modules** page at any time to **Delete** or **Deactivate** the rule.

### Configure Suspend Guard Protection

Suspend Guard protects against a common malware technique where the attacker creates processes in a suspended state and injects and runs code before the process even starts. When enabled, the Suspend Guard module protects all processes from Suspend Guard attacks and uses whitelists to permit common legitimate processes to inject into other processes or modules.

The default policy contains rules intended to prevent malicious injection and permits legitimate processes that must inject threads into other processes.
Use caution when configuring new Suspend Guard rules to avoid overriding the default policy and causing instability in your network.

For additional questions on configuring malware protection rules, contact the Support team or your Systems Engineer.

If the process is not already protected by the default security policy, you can create a new rule that enables Suspend Guard protection for a process using the default Suspend Guard settings or you can configure the settings as needed to meet the requirements of your security policy. Settings include the process name, Activation (On or Off), Action (Prevention or Notification), User Alert (On or Off), and whitelist function modules that can call child processes.

If the process is already protected by the default security policy, we recommend importing the default Suspend Guard policy as a new rule and making changes to meet the requirements of your organization. This ensures that, when the policy is activated, it overrides the default policy but still contains the default configuration settings in addition to any changes you made.

**STEP 1 | Configure a Suspend Guard rule.**

1. Perform one of the following actions:
   - Add a new rule.
   - Select and Edit an existing rule.
   - Review the default policy rules (select Show Default Rules from the action menu at the top of the table), select a rule, and then Clone it.
2. Select Suspend Guard.

**STEP 2 | (Optional) Define the Suspend Guard settings.**

To use the settings defined by the default policy, enable the module and then skip to 5.

1. From the Activation drop-down, select On to enable the rule or Off to disable the rule.

   Any additional settings are ignored if the malware protection module is disabled.

2. Configure the Action to take when a source process attempts to inject into another process:
   - Inherit—Inherit the behavior from the default policy.
   - Prevention—Terminate the process.
   - Notification—Log the issue and allow the process to inject into another process.
3. Configure the User Alert behavior when the source process attempts to inject into another process.
   - Inherit—Inherit the behavior from the default policy.
   - On—Notify the user when a process tries to inject into another.
   - Off—Do not notify the user when a process tries to inject into another.

**STEP 3 | (New rules only) Enable Suspend Guard protection for a single process or for all processes.**

To configure Suspend Guard protection for a parent process, select the option to Select a process and enter the process name in the field provided. Otherwise, keep the default setting to apply Suspend Guard protection to All Processes.

**STEP 4 | (Optional) Add a function and child process to a whitelist.** By default, when a Suspend Guard rule is enabled, Traps blocks all functions of the parent process from injecting into any child processes. To explicitly allow injection into functions and child processes, add them to a whitelist.
To avoid overriding the whitelist in the default malware protection policy, we highly recommend that you do not change the Whitelist Actions and, instead, keep the default Merge setting.

1. Click the ninja mode icon and enter the administrative password.
2. Inherit the default whitelist settings or Whitelist specific function and child processes. Configure the whitelist to allow any combination of the following:
   - All functions that inject into any child process
   - A specific function that injects into any child process
   - All functions that inject into a specific process
   - A specific function that injects into a specific process
   Repeat as needed to add multiple combinations per parent process.

STEP 5 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 6 | (Optional) Define the Target Objects to which to apply the malware protection rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 7 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 8 | Save the malware protection rule.

Do either of the following:
   - Save the rule. This option is only available for inactive, cloned, or new rules. To activate the rule later, select the rule from the Policies > Malware > Protection Modules page and then click Activate.
   - Apply the rule to activate it immediately.

After saving or applying a rule, you can return to the Policies > Malware > Protection Modules page at any time to Delete or Deactivate the rule.

Manage the Suspend Guard Whitelist

If a legitimate function module of a parent process must inject into a child process, use this workflow to explicitly allow the function module to inject into the child process as needed by adding the module or child process to a whitelist.

STEP 1 | Use the filter to locate the active Suspend Guard rule for a specific process.
This method of filtering rules only works if the Auto Description feature is turned on during rule creation or if you manually enter the process name into the rule description.

1. Select Policies > Malware > Protection Modules.
2. Select the filter icon for the Description column.
3. Set the Show item criteria to Contains and enter a process name in the field provided.
4. Select Filter.

STEP 2 | Modify the malware protection rule.
Select and then Edit the rule. If the rule doesn't exist, create it as described in Configure Suspend Guard Protection.

STEP 3 | Add a target process to a whitelist.
By default, the whitelist prevents all function modules of the parent process from injecting into any child processes. If a legitimate function module must inject into a child process, explicitly allow the injection by adding the module or child process to a whitelist.

1. Click the ninja mode icon ⚡ and enter the administrative password.
2. Add the name of the function module or child process to the whitelist in one of the following ways:
3. Configure the whitelist to allow any combination of the following:
   • All functions that inject into any child process
   • A specific function that injects into any child process
   • All functions that inject into a specific process
   • A specific function that injects into a specific process
   Repeat as needed to add multiple combinations per parent process.

STEP 4 | Save the malware protection rule.
Do either of the following:
   • Save the rule. This option is only available for inactive, cloned, or new rules. To activate the rule later, select the rule from the Policies > Malware > Protection Modules page and then click Activate.
   • Apply the rule to activate it immediately.

After saving or applying a rule, you can return to the Policies > Malware > Protection Modules page at any time to Delete or Deactivate the rule.
Exploit Protection

> Manage Processes
> Manage Exploit Protection Rules
Manage Processes

By default, the Endpoint Security Manager protects the most vulnerable and most commonly used processes in Windows environments. Details about these processes are available on the Process Management page and include information about the protection type, number of computers that run the process, and the date and time that the process was first discovered.

You can enable new process collection by enabling WildFire (see Set Up the ESM to Communicate with WildFire) or by creating an agent settings rule to collect new process information (see Collect New Process Information). As new executable files or processes are run on the endpoints, Traps reports them to the Endpoint Security Manager.

You can also add protection for other third-party and proprietary applications without collecting new process information by adding those applications directly to the list of protected processes on the Process Management page.

- Process Protection Types
- Processes Protected by the Default Policy
- Add a New Protected Process
- Import or Export a Process
- View, Modify, or Delete a Process
- View Processes Currently Protected by Traps

Process Protection Types

The ESM Console categorizes each process by a Protection Type:

- **Protected**—Indicates that the process is actively protected by exploit protection rules that apply to all processes. You can also configure process-specific rules that only apply to select processes.
- **Provisional**—Indicates that the process is undergoing a test run as a protected process, usually on a small number of endpoints and with a small number of rules. After the test run completes and you make any necessary adjustments to the associated rules, you can change the protection type of the process to Protected.
- **Unprotected**—A process is categorized as Unprotected when Traps first discovers a new process on an endpoint in your organization. Although your malware protection and WildFire policies automatically protect these processes, you must categorize new processes as Protected or Provisional processes to apply the exploit protection policy.

Processes Protected by the Default Policy

The Endpoint Security Manager and Traps come preconfigured to protect common applications and processes on Windows endpoints. These processes vary depending on the associated content update version. To determine which processes are supported in a given release, look up the content update version associated with the release (see Associated Software Versions) and then review the release notes for the content update on the Support portal.

The process type, as shown on the Process Management page, does not indicate whether a process is used in the default security policy. Instead, the process type only indicates whether the process can be used in an exploit protection rule. For more information, see Process Protection Types.
Add a New Protected Process

A process is an active instance of a program that is executed by the operating system. From the Windows Task Manager on the endpoint, you can view all active processes that are currently running including the names of core system processes. Many core system processes are protected by the operating system and cannot be renamed. Changing the name of these system process—for example, changing the name of the calc.exe process to calc1.exe—can cause the process to stop functioning. Because Traps identifies processes by name, changing the name of a process can also prevent Traps from applying protection rules to the new process name.

The ESM Console is preconfigured with a default exploit protection policy that protects the most vulnerable and most commonly used processes. You can protect additional uncommon, third-party, and proprietary processes by adding their names to the list of protected processes. Each rule in the exploit protection policy protects one or more processes from a specific type of exploit or vulnerability using exploit protection modules (EPMs). Depending on the configuration, Traps can activate the EPM in all processes or in specific process names. Adding a new process to the list of protected processes enables you to automatically protect the process-without any additional configuration-using any exploit protection rules that apply to all processes.

To ensure process protection continues, we recommend that you do not change the names of commonly used processes on the system. If a process name change is required, ensure that you add the renamed process as a protected process and mirror the protection rules for the old process name. As needed, you can also configure additional exploit protection rules to protect the process.

By extending protection to the applications that are important to your organization, you can provide maximum protection with minimal disruption of day-to-day activities. Add processes as either protected, provisional, or unprotected and configure them using the Process Management page.

You can configure only exploit protection rules on Protected or Provisional processes.

You cannot change the default Protected processes that are included in the initial setup. Consult the Palo Alto Networks support team for questions.

STEP 1 | Navigate to the Process Management page.
From the ESM Console, select Policies > Exploit > Process Management.

STEP 2 | Add a new process.
1. Click Add.
2. Enter the Process name.
3. To actively protect the process using default and user-defined rules, set the Protection type to Protected. For additional options, see Process Protection Types.

**STEP 3 |** Save your changes to the process.

Click Create.

**STEP 4 |** For each new protected process, configure an exploit protection rule to activate the ROP Mitigation EPM in the process and another exploit protection rule to activate the JIT Mitigation EPM in the process. These exploit protection rules provide the best protection with the lowest false-positive rate.

1. For each EPM, Create an Exploit Protection Rule with the following settings:

   **EPM:**
   - **Activation**—Inherit
   - **Action**—Notification
   - **User Alert**—Off

   **Processes:**
   - Select the new protected process.

   **Objects:**
   - To identify any unintended consequences of protecting the new process, select a small number of endpoints. If you have different environments within your organization (for example, different operating systems), we recommend that you select a few endpoints in each environment.

2. Apply the rule and then repeat the process for the second EPM.

3. After a period in which no issues are caused by the new rules, update and then apply the rule settings:

   **EPM:**
   - **Action**—Prevention
   - **User Alert**—On

   **Objects:**
   - Expand the rule deployment: Add additional objects or remove all objects. In the case of the latter, if no objects are specified, the rule applies to all endpoints.

**Import or Export a Process**

Use the export and import features in the ESM Console to back up one or more process definitions used in your security policy. The export and import features allow you to back up processes before migrating or upgrading to a new server, or deploying a managed process to multiple independent servers. You can export processes on a global or individual basis and save them to an XML file. The import feature appends imported processes to the existing list of default and added processes and also displays their protection types.

**STEP 1 |** Navigate to the Process Management page.

From the ESM Console, select Policies > Exploit > Process Management.

**STEP 2 |** Import or export one or more processes.
• To import processes, click the action menu ➞ and then select Import Processes. Browse to and Upload the file containing details about processes you want to import. The processes appear in the table after the upload is complete.
• To export processes, select one or more processes that you want to export. From the action menu ➞ ., select Export Selected. The ESM Console saves the processes to an XML file.

View, Modify, or Delete a Process

The Processes Management page in the ESM Console displays all the processes that your organization's security policy protects. To change or delete a process, you must first remove the process from any associated rules.

STEP 1 | Navigate to the Process Management page.
From the ESM Console, select Policies > Exploit > Process Management.

STEP 2 | View the processes in the Process Management table.
Use the paging controls at the top of the table to view different portions of the table.
The following fields are displayed:
• Process—Filename of the process executable file.
• Protection Type—Protected, Unprotected, or Provisional.
• Computers—Number of endpoints on which the process has run.
• Linked Rules—Number of rules configured for the process.
• Discovered On—Name of the endpoint on which the process was first discovered.
• First Seen—Date and time the process was first discovered on the endpoint (after receiving a rule to report new processes).

STEP 3 | Delete or change the process.
If the process is used in any rules, you must first unlink (remove) the process from the rule. After the process is unlinked, you can select the name of the process and do any of the following:
• Delete the process.
• Change the Process Name and then Save your changes.
• Change the Protection Type and then Save your changes. For more information, see Process Protection Types.

View Processes Currently Protected by Traps

When a user creates or opens a protected process on an endpoint, the Traps agent injects a protection module, called an Exploitation Protection Module (EPM), into the process. The endpoint security policy rules determine which EPMs are injected into which processes.

You can view processes that are currently protected by Traps using either the Traps Console or a command-line interface called Cytool (see View Processes Currently Protected by Traps Using Cytool).

The Protection tab on the Traps Console displays processes that are currently protected by Traps.
For each process, Traps displays the name, description, unique ID number, time the process was initiated, and memory allocation register.

**STEP 1 | Launch the Traps Console:**

- From the Windows tray, double-click the Traps icon or right-click the icon and select **Console**.
- Run CyveraConsole.exe from the Traps installation folder.

The Traps Console launches.

**STEP 2 | Select the **Advanced** > **Protection** tab to view the protected processes.**
Manage Exploit Protection Rules

- Exploit Protection Rules
- Exploit Protection Rule Hierarchy
- Exploit Protection Modules (EPMs)
- Default Exploit Protection Policy
- Create an Exploit Protection Rule
- Exclude an Endpoint from an Exploit Protection Rule

Exploit Protection Rules

An exploit protection rule uses Exploit Protection Modules (EPMs) to protect processes in your organization from specific exploitation techniques. An EPM is a code module that you activate for one or more processes to prevent attacks on program vulnerabilities related to memory corruption or logic flaws.

The Default Exploit Protection Policy contains a preconfigured set of exploit protection rules that are activated for commonly used protected processes. To protect processes and additional applications that are important to your organization, you can add these to the list of protected or provisional processes and then configure additional exploit protection rules. For example, to protect two processes that your organization uses (for example, ProcessA.exe and ProcessB.exe) from a specific type of memory corruption attack called return oriented programming (ROP), you can add the processes to the protected processes list and then create an exploit protection rule that activates the ROP Mitigation EPM. When a user opens a file or URL, the Traps agent injects code into the protected process or processes involved in opening the file and activates the EPM. If the file contains code designed to exploit APIs used in ROP chains, Traps blocks the memory corruption attack. When a security event triggers a prevention, the Traps agent also takes a snapshot of the memory for subsequent forensic investigation.

On a regular basis, the Traps agent retrieves the latest security policy from the ESM Server. The security policy determines which processes Traps protects and the type of EPM that Traps activates to protect the process.

View a summary of exploit protection rules on the Policies > Exploit > Protection Modules page. Selecting a rule on the page displays further information about the rule and other actions that you can take on the rule (Delete, Activate/Deactivate, or Edit). For more information, see Manage Exploit Protection Rules.

Consult with Palo Alto Networks Support before making any changes to the EPMs in security policy rules.

Exploit Protection Rule Hierarchy

When new exploit protection rules are added to the security policy, the Traps rules mechanism merges all configured rules into an effective policy that is evaluated for each endpoint. In the case of a potential conflict between two or more rules, Traps uses the following considerations to determine which rule takes effect:

- **Process specificity**—The more specific a rule, the higher the priority. For example, a rule configured for a specific process takes precedence over a rule configured for all processes.
- **Modification date**—A rule that was created or edited more recently takes precedence over an older rule.

Exploit Protection Modules (EPMs)

The following table describes the types of EPMs and the type of exploit that each module protects against:
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPL Protection</td>
<td>Software logic flaw</td>
<td>Protects against vulnerabilities related to the display routine for Windows Control Panel shortcut images, which can be used as a malware infection vector.</td>
</tr>
<tr>
<td>DEP</td>
<td>Memory corruption</td>
<td>Data execution prevention (DEP). Prevents areas of memory designated as containing data from running as executable code.</td>
</tr>
<tr>
<td>DLL Security</td>
<td>Memory corruption</td>
<td>Prevents access to crucial DLL metadata from untrusted code locations.</td>
</tr>
<tr>
<td>DLL-Hijacking Protection</td>
<td>Software logic flaw</td>
<td>Prevents DLL-hijacking attacks where the attacker attempts to load DLLs from unsecured locations to gain control of a process.</td>
</tr>
<tr>
<td>Exception Heap Spray Check</td>
<td>Memory corruption</td>
<td>Detects instances of heap sprays upon occurrence of suspicious process crashes (indicative of exploitation attempts).</td>
</tr>
<tr>
<td>Font Protection</td>
<td>Software logic flaw</td>
<td>Prevents improper font handling, a common target of exploits.</td>
</tr>
<tr>
<td>Hot Patch Protection</td>
<td>Software logic flaw</td>
<td>Prevents the use of system functions to bypass DEP and address space layout randomization (ASLR).</td>
</tr>
<tr>
<td>JIT Mitigation</td>
<td>Memory corruption</td>
<td>Prevents an attacker from bypassing the operating system's memory mitigations using just-in-time (JIT) compilation engines. In ninja-mode, you can also configure advanced hooks and whitelists for this module.</td>
</tr>
<tr>
<td>Library Preallocation</td>
<td>Memory corruption</td>
<td>Enforces relocation of specific modules that exploitation attempts commonly utilize.</td>
</tr>
<tr>
<td>Memory Limit Heap Spray Check</td>
<td>Memory corruption</td>
<td>Detects instances of heap sprays using the Palo Alto Networks proprietary algorithm, which is triggered by a sudden increase in memory consumption (indicative of ongoing exploitation).</td>
</tr>
<tr>
<td>Null Dereference Protection</td>
<td>Memory corruption</td>
<td>Prevents malicious code from mapping to address zero in the memory space, making null dereference vulnerabilities unexploitable.</td>
</tr>
<tr>
<td>ROP Mitigation</td>
<td>Memory corruption</td>
<td>Protects against the use of return oriented programming (ROP) by protecting APIs used in ROP chains.</td>
</tr>
<tr>
<td>SEH Protection</td>
<td>Memory corruption</td>
<td>Prevents hijacking of the Structured Exception Handler (SEH), a commonly exploited control structure called Linked List, which contains a sequence of function records.</td>
</tr>
<tr>
<td>Shellcode Preallocation</td>
<td>Memory corruption</td>
<td>Reserves and protects certain areas of memory commonly used to house payloads using heap spray techniques.</td>
</tr>
<tr>
<td>ShellLink Protection</td>
<td>Software logic flaw</td>
<td>Prevents shell-link logical vulnerabilities.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SysExit</td>
<td>Memory corruption</td>
<td>Protects against the use of return oriented programming (ROP) by protecting APIs used in ROP chains.</td>
</tr>
<tr>
<td>UASLR</td>
<td>Memory corruption</td>
<td>Improves or altogether implements ASLR (module location randomization) with greater entropy, robustness, and strict enforcement.</td>
</tr>
</tbody>
</table>

**Default Exploit Protection Policy**

By default, the Endpoint Security Manager security policy contains Exploit Protection Rules that are enabled to protect against attacks that leverage common software vulnerabilities and exploits. The following table describes the default exploit protection policy settings. When configuring new exploit protection rules, you can inherit the default behavior shown in the Mode and User Notification column or you can override the settings to meet the requirements of your organization's security policy. To configure advanced EPMs and EPM settings, you must enter the ninja mode password.

<table>
<thead>
<tr>
<th>EPM</th>
<th>Enabled by Default?</th>
<th>Mode</th>
<th>User Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPL Protection</td>
<td>✓</td>
<td>Notification</td>
<td>On</td>
</tr>
<tr>
<td>DEP</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>DLL Security</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>DLL-Hijacking Protection</td>
<td></td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Exception Heap Spray Check</td>
<td></td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Font Protection</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Hot Patch Protection</td>
<td></td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>JIT Mitigation</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Library Preallocation</td>
<td></td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Memory Limit Heap Spray Check</td>
<td></td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Null Dereference Protection</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>ROP Mitigation</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>SEH Protection</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
<tr>
<td>Shellcode Preallocation</td>
<td>✓</td>
<td>Prevention</td>
<td>On</td>
</tr>
</tbody>
</table>
Create an Exploit Protection Rule

An exploit protection rule uses Exploit Protection Modules (EPMs) to protect processes in your organization from specific exploitation techniques.

Create an exploit protection rule to define the specific module used to protect commonly used processes in your organization. Each module prevents attempts to exploit program vulnerabilities related to memory corruption and software logic flaws and protects against a specific attack method, such as DLL hijacking or heap corruption. Activate an EPM module to protect one or more processes that may be vulnerable to a specific type of attack.

For each exploit protection rule you add, configure EPM-specific settings and choose the process or processes to which the rule applies (you can specify a single process, multiple processes, or all processes). Typically, these settings include EPM activation, Traps behavior, and user notification.

As with other types of rules, you can reduce the scope of an exploit protection rule by specifying Target Objects and Conditions that must be satisfied for the rule to apply. A target object can be any user, group, organizational unit, or computer that appears in Active Directory or any existing endpoint on which the Traps agent is installed. A condition can refer to a specific file, the specific version or range of versions for a file, or a registry path that must exist on the endpoint.

Additional EPMs and fine-grained settings are hidden and are only accessible in ninja mode ☢️. To configure these EPMs and settings, you must enter an administrative password.
Configuring exploit protection rules is an advanced feature. To change or override an exploit protection rule, consult with the Palo Alto Networks support team.

STEP 1 | Configure a new exploit protection rule.
Select Policies > Exploit > Protection Modules and then Add a new rule.

STEP 2 | Configure EPM injection.
By default, EPM injection is enabled. To disable all exploit protection of the protected processes on your system, select the option at the bottom of the list of EPMs to Disable All EPM Injection.

STEP 3 | Configure the settings for the EPM module.
1. Select the EPM from the list and configure its settings in the Details section. The settings for each type of EPM are different but can include preferences on whether or not to terminate a process and notify a user about a security event.
2. Repeat the process to add and configure additional EPMs. For more information on the different types of EPMs, see Exploit Protection Rules.

Changing EPM definitions changes the order in which rules are evaluated and can affect your protection level (see Policy Enforcement). To avoid compromising your organizational security, consult with Palo Alto Networks Support.

STEP 4 | Select the processes for which you want to apply the rule.
Before configuring an exploit protection rule on a new process, you must define the process and the protection type on the Policies > Exploit > Process Management page. To add a new process, see Add a New Protected Process. To change the protection type of a process, for example from Unknown to Protected, see View, Modify, or Delete a Process.

1. Select the Processes tab.
2. Narrow the list of processes by selecting the process type from the drop-down, either Protected or Provisional. Provisional processes are processes that are undergoing a test run and are monitored separately from protected processes. For a list of processes that are protected by the default security policy, see Default Protected Processes.
3. Select one or more processes to which to apply the rule, and then click Add. Or, to apply the rule to all protected or provisional processes, select All Processes.

STEP 5 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.
To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 6 | (Optional) Define the Target Objects to which to apply the restriction rule.
To define a smaller subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas.
The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 7 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.
To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.
STEP 8 | Save the exploit protection rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Policies > Exploit > Protection Modules page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Protection Modules page at any time to **Delete** or **Deactivate** the rule.

Exclude an Endpoint from an Exploit Protection Rule

When an endpoint attempts to launch an application that violates an exploit protection policy, the Traps agent stops the process from running and reports the malicious process to the Endpoint Security Manager. The Security Events > Threats page provides detailed information about processes that trigger security events and the Exploit Protection Modules (EPMs) that prevent the attacks.

To allow the process to run on a specific endpoint without deleting or disabling the policy rule, create an exclusion rule based on the security event details. Defining an exclusion rule disables the EPM that prevented the process from running on a specific endpoint.

-To avoid unnecessarily exposing your organization to attacks, create exclusion rules only when necessary.-

You can also create exclusion rules from scratch by adding Objects to the Exclude section of the rule (see Create an Exploit Protection Rule).

STEP 1 | Launch the Threats page.
- From the ESM Console, select Security Events > Threats.

STEP 2 | Select the event.
- Select the security event for which you want to create the exclusion rule. The event expands to display further details and actions about the security event.

STEP 3 | Create an exclusion rule.
- By default the exclusion rule applies only to the endpoint on which the security event occurred. If you want to exclude multiple objects or endpoints from the rule, add them to the Exclude section on the Objects tab.
  1. Click **Create** to populate the rule with details about the specific EPM and endpoint. The button is only available for exploit protection rules.
  2. If needed, review the details on the Processes, Conditions, Objects, and Name tabs.
  3. **Apply** the rule immediately or **Save** the rule to activate it later.

STEP 4 | Verify that the exclusion rule allows the process to run on the endpoint.
- 1. Open the Traps Console.
  2. Select **Check-in now** to request the latest security policy.
  3. Select Advanced > Policy and verify that the rule appears.
  4. Launch the application on the endpoint to verify that the user can successfully run the process.
Manage the Endpoints

The following topics describe how to manage the endpoints using the Endpoint Security Manager:

- Manage Traps Action Rules
- Manage Agent Settings Rules
Manage Traps Action Rules

Use action rules to perform one-time actions on the Traps agent that runs on each endpoint.

- Traps Action Rules
- Add a New Action Rule
- Manage Data Collected by Traps
- Uninstall or Upgrade Traps on the Endpoint
- Update or Revoke the Traps License on the Endpoint

Traps Action Rules

Action rules enable you to perform one-time actions on the Traps agent that runs on each endpoint. For each action rule, you must specify target object(s), condition(s), and one of the following administrative actions to take on each endpoint:

<table>
<thead>
<tr>
<th>Action Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage data files that the Traps agent</td>
<td>Each endpoint stores prevention and security information that includes historical data, memory dumps, and quarantined files. Using this type of action rule, you can erase or retrieve data files that the Traps agent creates on the endpoint. For more information, see Manage Data Collected by Traps.</td>
</tr>
<tr>
<td>Uninstall or upgrade the Traps software</td>
<td>Create an action rule to uninstall or upgrade Traps from the Endpoint Security Manager. To upgrade the Traps software on an endpoint, upload the software zip file to the ESM (ESM) Server and specify the path when configuring the action rule. For more information, see Uninstall or Upgrade Traps on the Endpoint.</td>
</tr>
<tr>
<td>Update or revoke the Traps license</td>
<td>The Endpoint Security Manager distributes licenses to the Traps agent. You can revoke or update that license on an endpoint at any time. For more information, see Update or Revoke the Traps License on the Endpoint.</td>
</tr>
</tbody>
</table>

Traps does not apply action rules until the Traps agent receives the updated security policy, typically with the next heartbeat communication with the server. To manually retrieve the latest security policy from the ESM Server, select Check-in now on the Traps Console.

You can create or edit action rules on the Actions summary and management page (Settings > Agent > Actions). Select a rule to display additional information about that rule and other actions that you can take on the rule (Duplicate, Delete, or Activate/Deactivate). For more information, see Manage Traps Action Rules.

Add a New Action Rule

For each action rule, you can specify organizational objects, conditions, and actions to take on each endpoint.

STEP 1 | Create a new action rule.
Select Settings > Agent > Actions and then Add a new rule.

**STEP 2 |** Select the type of task you want to perform.

Select one of the following action rule types and then configure the settings according to the type of action:

- **Agent Data**— For more information, see Manage Data Collected by Traps.
- **Agent Installation**— For more information, see Uninstall or Upgrade Traps on the Endpoint.
- **Agent License**— For more information, see Update or Revoke the Traps License on the Endpoint.

**STEP 3 |** (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat this step to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

**STEP 4 |** (Optional) Define the Target Objects to which to apply the action rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5 |** (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

**STEP 6 |** Save the action rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Actions page and then click Activate.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Actions page at any time to Delete or Deactivate the rule.

**Manage Data Collected by Traps**

To manage data collected by Traps, you can configure an action rule that runs only one time on the endpoint; after the Traps agent performs the action once, it will not repeat the action. To perform the same action again, Duplicate the action from the Settings > Agent > Actions page.

**STEP 1 |** Create a new action rule.

Select Settings > Agent > Actions and then Add a new rule.

**STEP 2 |** Configure the tasks you want to perform on the Traps data stored on the endpoints.

Select Agent Data and then select any of the following options to manage Traps agent data.
• **Clear history**—Each endpoint stores a history of security prevention events. Select this option to clear historical data files from the Traps Console.

• **Erase memory dumps**—Memory dumps are records of the contents of system memory when a prevention event occurs. Select this option to erase the system memory records from target objects.

• **Erase quarantined files**—When a security event occurs on an endpoint, Traps captures memory dumps and recent files associated with the event and stores (quarantines) them in the forensic folder on the endpoint. Select this option to delete the files associated with the security event from the target objects.

• **Retrieve collected data from the agent**—Traps collects security event history, memory dumps, and other information associated with a security event. Select this option to retrieve all the information saved from all events that occurred on the endpoint. After this rule runs, the Traps agent sends all the data related to the prevention event, including a memory dump of the protected process, to the designated forensic folder.

• **Retrieve collected logs from the agent**—Traps collects detailed application trace logs and stores information about processes and applications that run on the endpoint. Use the log file to debug an issue with an application or investigate a specific problem captured in the log. Select this option to create an action rule that retrieves all the application trace information for an endpoint. After this rule runs, the Traps agent sends all the logs to the forensic folder.

**STEP 3 | (Optional) Add Conditions to the rule.** By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 4 | (Optional) Define the Target Objects** to which to apply the action rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5 | (Optional) Review the rule name and description.** The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6 | Save the action rule.**

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Settings > Agent > Actions** page and then click **Activate**.

- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Actions** page at any time to **Delete** or **Deactivate** the rule.

**STEP 7 | Next steps...**

- **View the status of the rule**—After creating the action rule, you can view its status from the **Actions** page. The status displays the number of agents that successfully completed the action and the number of agents that failed to complete the action.
• **Duplicate the rule**—From the Actions page, select the rule and click Duplicate. The ESM Console uses the settings from the rule you selected to populate a new rule. You can then change the scope of the rule by applying it to different target objects or leave it as is to run it again with the same settings; Then, Save or Apply the rule as described in the previous step.

• **Retrieve data**—If you created an action rule to retrieve data from the endpoint, select Monitor > Data Retrieval to view the Upload State of all data uploads. After the Traps agent completes the data upload, this page displays the event along with a link which allows you to Download the data.

**Uninstall or Upgrade Traps on the Endpoint**

Create a new agent actions rule to uninstall Traps from the target objects or upgrade Traps using software that is accessible by the ESM Console.

**STEP 1** | Create a new action rule.
Select Settings > Agent > Actions and then Add a new rule.

**STEP 2** | Define the tasks you want to perform on the Traps agent on the endpoints.
1. Select Agent Installation and then select Uninstall to uninstall the Traps software or Upgrade from path to browse to and then select the installation file to use for upgrading the Traps software.
2. Enter the Uninstall Password.

**STEP 3** | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.
To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

**STEP 4** | (Optional) Define the Target Objects to which to apply the action rule. By default, a new rule applies to all objects in your organization.
To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5** | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.
To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

**STEP 6** | Save the action rule.
Do either of the following:

• **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Actions page and then click Activate.

• **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Actions page at any time to Delete or Deactivate the rule.
Update or Revoke the Traps License on the Endpoint

Create a new action rule to update or revoke a license for a Traps agent on an endpoint.

When using an action rule to revoke a license, the Traps agent performs that action at the next heartbeat communication with the ESM Server. After the action rule runs on the endpoint, Traps stops protecting the endpoint and allows the ESM Server to reallocate the license to another Traps agent. When the endpoint or Traps service restarts (such as after a reboot), the agent requests a new license from the ESM Server. To resume Traps protection, you must create a new action rule to update the license for the Traps agent.

In an urgent situation that requires an immediate release of the license from the database, you can Detach a Traps License without waiting for the next heartbeat communication.

STEP 1 | Create a new action rule.
Select Settings > Agent > Actions and then Add a new rule.

STEP 2 | Define the tasks you want to perform on the Traps license on the endpoints.
Select Agent License and then select either of the following actions:
- **Update**—Update the Traps license on an endpoint.
- **Revoke**—Revoke a license and stop the Traps agent service on an endpoint.

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.
To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the Target Objects to which to apply the action rule. By default, a new rule applies to all objects in your organization.
To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.
To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the action rule.
Do either of the following:
- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Actions page and then click Activate.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Actions page at any time to Delete or Deactivate the rule.
Manage Agent Settings Rules

Create *agent settings rules* from a central location to change preferences related to Traps.

- Traps Agent Settings Rules
- Add a New Agent Settings Rule
- Define Event Logging Preferences
- Hide or Restrict Access to the Traps Console
- Define Communication Settings Between the Endpoint and the ESM Server
- Collect New Process Information
- Manage Service Protection
- Change the Uninstall Password
- Create a Custom User Alert Message

### Traps Agent Settings Rules

Agent settings rules enable you to change preferences related to Traps from a central location. From the **Settings > Agent > Settings** page, you can create rules to manage the following Traps settings:

<table>
<thead>
<tr>
<th>Agent Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event logging</td>
<td>Configure a size quota for endpoint logs. For more information, see Define Event Logging Preferences.</td>
</tr>
<tr>
<td>User visibility and access</td>
<td>Determine whether and how end users can access the Traps Console application. Optionally, you can configure the console so that only administrators can access it. For more information, see Hide or Restrict Access to the Traps Console.</td>
</tr>
<tr>
<td>Heartbeat frequency</td>
<td>Determine the frequency at which the Traps agent sends a heartbeat message to the ESM Server. The optimal frequency is determined according to the number of endpoints in the organization and the typical network load. For more information, see Define Heartbeat Settings Between the Agent and the ESM Server.</td>
</tr>
<tr>
<td>New process information collection</td>
<td>Configure Traps agents to collect new processes from endpoints. When this option is enabled, Traps reports every new process that runs on an endpoint to the ESM Server. You can view the processes in the Process Management view of the ESM Console and choose whether to create security rules related to the processes. For more information, see Collect New Process Information.</td>
</tr>
<tr>
<td>Service protection</td>
<td>Prevent attempts to disable or make changes to the Traps registry values and files. When this option is enabled, users cannot shut down or modify the Traps agent service. For more information, see Manage Service Protection.</td>
</tr>
<tr>
<td>Agent security</td>
<td>By default, users and administrators must enter a password to uninstall the Traps application. Use this option to change the password. For more information, see Change the Uninstall Password.</td>
</tr>
<tr>
<td>Agent Settings</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Communication</td>
<td>Configure the amount of time, known as the timeout value, after which Traps stops initiating attempts to reconnect to the ESM Server when the server becomes unreachable. Configure the grace period to specify when Traps should attempt to reestablish communication. For more information, see Define Communication Settings Between the Agent and the ESM Server.</td>
</tr>
<tr>
<td>User alerts</td>
<td>Customize the general settings for all user alerts, including the display image and footer. You can also configure the title that appears on user alerts related to protection modules, restrictions, and unknown files. For more information, see Create a Custom User Alert Message.</td>
</tr>
</tbody>
</table>

Traps does not apply agent setting rules until the Traps agent receives the updated security policy, typically with the next heartbeat communication with the server. To manually retrieve the latest security policy from the ESM Server, select Check-in now on the Traps Console.

Select a rule on the Settings page to display additional information about that rule and other actions that you can perform to manage the rule (Delete, Activate/Deactivate, or Edit). For more information, see Manage Agent Settings Rules.

Add a New Agent Settings Rule

For each agent settings rule, you can specify organizational objects, conditions, and Traps preferences to apply.

STEP 1 | Create a new agent settings rule.

Select Settings > Agent > Settings and then Add a new rule.

STEP 2 | Select the type of setting that you want to change and configure your preferences.

Select one of the following, and then configure the settings according to the type of preference:

- **Event Logging**—For more information, see Define Event Logging Preferences.
- **User Visibility & Access**—For more information, see Hide or Restrict Access to the Traps Console.
- **Heartbeat Settings**—For more information, see Define Heartbeat Settings Between the Agent and the ESM Server.
- **Process Management**—For more information, see Collect New Process Information.
- **Service Protection**—For more information, see Manage Service Protection.
- **Agent Security**—For more information, see Change the Uninstall Password.
- **Communication Settings**—For more information, see Define Communication Settings Between the Agent and the ESM Server.
- **User Alerts**—For more information, see Create a Custom User Alert Message.

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.
STEP 4 | (Optional) Define the Target Objects to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the agent settings rule.

Do either of the following:

- Save the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Settings page and then click Activate.
- Apply the rule to activate it immediately.

After saving or applying a rule, you can return to the Settings page at any time to Delete or Deactivate the rule.

Define Event Logging Preferences

Traps stores event information and quarantined files in a temporary local storage folder. To adjust the size of the disk quota, configure an agent settings rule:

STEP 1 | Create a new agent settings rule.

Select Settings > Agent > Settings and then Add a new rule.

STEP 2 | Define the event logging settings for the endpoints.

1. Select Event Logging.
2. Select Set disk quota (MB) and specify the size of the temporary local storage folder that Traps will use to store event logs and quarantined files. Specify the quota amount in MB (default is 5,120; range is 0 to 10,000,000). After the storage folder reaches the size quota, Traps purges the event logs by deleting the oldest logs first to make room for new logs.

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the Target Objects to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.
STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the agent settings rule.

Do either of the following:

• Save the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Settings page and then click Activate.

• Apply the rule to activate it immediately.

After saving or applying a rule, you can return to the Settings page at any time to Delete or Deactivate the rule.

Hide or Restrict Access to the Traps Console

By default, a user can access the Traps Console to view information about the current status of the endpoint, changes to the security policy, and any security events. When a security event is triggered, the user also receives a notification about the event. The notification includes the application name, the publisher, and a description of the exploit prevention or restriction rule that triggered the notification.

You can create an agent settings rule to change the accessibility of the console and specify whether to hide notifications from users.

STEP 1 | Create a new agent settings rule.

Select Settings > Agent > Settings, and then Add a new rule.

STEP 2 | Define user visibility and access for the endpoints.

Select User Availability & Access and then select one or more of the following options:

• Hide tray icon—Hide the tray icon which Traps otherwise adds to the notification area (system tray) on the endpoint.

• Disable access to the Traps console—Disable the ability to open the console.

• Hide Traps user notifications—Hide notifications that Traps otherwise displays when the agent encounters a prevention or notification event.

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.
**STEP 4** *(Optional)* Define the **Target Objects** to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users, Computers, Groups, Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5** *(Optional)* Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6** Save the agent settings rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Settings > Agent > Settings** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Settings** page at any time to **Delete** or **Deactivate** the rule.

**Define Communication Settings Between the Endpoint and the ESM Server**

The Traps agent on the endpoint communicates with the ESM Server at specific intervals by sending heartbeat messages and reports and by querying for unknown hash verdicts. Traps stops trying to reach the server if communication attempts fail for a period of time that exceeds a timeout value and Traps resumes attempts to reestablish communication with the server after a grace period.

To modify the default values for the heartbeat cycle, reports interval, timeout value, and/or grace period, create an agent settings rule on the ESM Console using the following workflows:

- **Define Heartbeat Settings Between the Agent and the ESM Server**
- **Define Communication Settings Between the Agent and the ESM Server**

**Define Heartbeat Settings Between the Agent and the ESM Server**

During the heartbeat communication, the Traps agent requests the current security policy and sends a response to the Endpoint Security Manager to report the status of the endpoint. The frequency at which the Traps agent sends heartbeat messages to the ESM Server is called the heartbeat cycle. The optimal frequency is determined according to the number of endpoints in the organization and the typical network load.

Traps also reports changes in service, including start, stop, and crash events and new processes discovered on the endpoint. The frequency at which the Traps agent sends report notifications is called the reports interval.

**STEP 1** Create a new agent settings rule.

Select **Settings > Agent > Settings** and then **Add** a new rule.

**STEP 2** Define the frequency of heartbeat messages and/or report notifications.
Select **Heartbeat Settings** and then configure either or both of the following settings:

- **Set distinct heartbeat cycle**—Modify the frequency (in minutes) at which Traps sends heartbeat messages to the ESM Server. Range is 0-144,000; Default is 60.
- **Set send reports interval**—Modify the frequency (in minutes) at which the Traps agent sends report notifications, including changes in service, crash events, and new processes. Range is 0-144,000; Default is 480 (8 hours).

**STEP 3** | *(Optional)* Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 4** | *(Optional)* Define the **Target Objects** to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users, Computers, Groups, Organizational Unit, or Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5** | *(Optional)* Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6** | Save the agent settings rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Settings > Agent > Settings** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Settings** page at any time to **Delete** or **Deactivate** the rule.

**Define Communication Settings Between the Agent and the ESM Server**

By default, the Traps agent applies a No Connection policy to all unknown executable files upon startup. The policy remains in place until the Traps agent can perform the ESM Server discovery to build a list of available servers in order of shortest path.

After the Traps agent builds the list of available servers and a user opens an unknown executable file, Traps queries the first ESM Server in the list to determine the hash verdict. If that server is unreachable or is unable to respond to the request within the maximum allotted time, the Traps agent stops trying to reach the ESM Server and assigns the executable file a No Connection verdict. If the user opens another unknown executable file before Traps determines that the ESM Server is unavailable, it will also query the first ESM Server in the list to determine the hash verdict. However, if the user opens another unknown executable file after the Traps agent determines that the ESM Server is unavailable, Traps will query the next ESM Server in the list.
The Traps agent also periodically polls the ESM server list to determine which servers are available and, of those available, which servers are closest. Other events, such as an IP address change on the endpoint, can also trigger Traps to rebuild the list of ESM Servers.

Use the following workflow to change the timeout and intervals for establishing communication with the ESM Server.

**STEP 1 |** Create a new agent settings rule.

Select **Settings > Agent > Settings** and then **Add** a new rule.

**STEP 2 |** Define the communication settings between the Traps agent and the ESM Server.

Select **Communication Settings** and then select one or more of the following options:

- **Set Agent-WildFire Process Verdict Timeout**—Specify the amount of time (in seconds) that Traps will wait for the ESM Server to respond to a verdict request (default is 10). After the timeout period expires, Traps assigns the process a **No Connection** verdict. Traps will attempt to reestablish communication only if a user clicks **Check-In Now** on the Traps Console, or if Traps needs to query the ESM Server for unknown hash verdicts.

  *If your endpoints frequently lose their connection with the server, consider increasing the timeout value.*

- **Set No Connection Refresh Interval**—Specify the frequency (in minutes) at which the Traps agent checks for available ESM Servers after entering a **No Connection** state (default is 1).

- **Set ESM Server Validation Interval**—Specify the frequency (in hours) at which the agent will verify the integrity of the ESM Server list (default is 1).

**STEP 3 |** (Optional) Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 4 |** (Optional) Define the **Target Objects** to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas.

The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5 |** (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6 |** Save the agent settings rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Settings > Agent > Settings** page and then click **Activate**.

- **Apply** the rule to activate it immediately.
After saving or applying a rule, you can return to the **Settings** page at any time to **Delete** or **Deactivate** the rule.

**Collect New Process Information**

By default, Traps protects the most commonly used and well-known processes on your endpoints. In addition, when WildFire is enabled, Traps automatically reports unknown executable files to the Endpoint Security Manager. If WildFire is disabled, it is recommended to create an agent settings rule to enable Traps to collect the names of any new processes that are run on the endpoints and report them to the Endpoint Security Manager. The ESM Console displays the processes as **Unprotected** on the **Process Management** page.

**STEP 1 | Create a new agent settings rule.**

Select **Settings > Agent > Settings** and then **Add** a new rule.

**STEP 2 | Enable the collection of new processes on the endpoints.**

Select **Process Management** and then enable the option to **Collect new process information**.

When Traps detects new processes, Traps reports the processes to the ESM Server. The ESM Console lists the new processes on the **Policies > Exploit > Process Management** page as unprotected processes. From there you can change the protection type (see **View, Modify, or Delete a Process**). After changing the protection type, you can then use it to **Create an Exploit Protection Rule**.

**STEP 3 | (Optional) Add Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

**STEP 4 | (Optional) Define the Target Objects** to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users, Computers, Groups, Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5 | (Optional) Review the rule name and description.** The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6 | Save the agent settings rule.**

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Settings > Agent > Settings** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Settings** page at any time to **Delete** or **Deactivate** the rule.
STEP 7 | On a regular basis, review the list of unprotected processes and evaluate whether add them to existing security rules or create new rules to protect them.
   2. Filter or sort the table by the Unprotected protection type.
   3. Review each process and decide whether to change the protection type:
      - Change the protection type to Provisional, if you want to use the process in a security rule run as a test.
      - Change the protection type to Protected to take advantage of existing rules that apply to all processes. See View, Modify, or Delete a Process. You can also add the process to rules that apply to specific processes, as needed.

Manage Service Protection

Service protection allows you to protect the Traps service running on your endpoints. When service protection is enabled, users cannot change registry values or files associated with the Traps agent and cannot stop or modify the Traps service in any way.

STEP 1 | Create a new agent settings rule.
   Select Settings > Agent > Settings and then Add a new rule.

STEP 2 | Enable service protection.
   Select Service Protection and then choose either of the following options:
      - Enable service protection
      - Disable service protection

STEP 3 | (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.
   To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

STEP 4 | (Optional) Define the Target Objects to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.
   To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.
   To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the agent settings rule.
   Do either of the following:
      - Save the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Settings page and then click Activate.
      - Apply the rule to activate it immediately.
After saving or applying a rule, you can return to the Settings page at any time to Delete or Deactivate the rule.

Change the Uninstall Password

By default, you must enter the uninstall password specified during installation to uninstall Traps from an endpoint. Change the default password by creating an agent settings rule.

**STEP 1 |** Create a new agent settings rule.

Select Settings > Agent > Settings and then Add a new rule.

**STEP 2 |** Change the password.

1. Select Agent Security and then select the option to Set uninstall password.
2. Enter the password that the user or administrator must enter to uninstall Traps. The password must be at least eight characters long.

**STEP 3 |** (Optional) Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

**STEP 4 |** (Optional) Define the Target Objects to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.

To define a subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Units, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5 |** (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

**STEP 6 |** Save the agent settings rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the Settings > Agent > Settings page and then click Activate.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the Settings page at any time to Delete or Deactivate the rule.
Create a Custom User Alert Message

Traps displays prevention and notification messages when a file or process violates a security policy and the termination behavior is configured to block the file and notify the user or to log the issue and notify the user. Use an agent settings rule to customize the general settings for all user alerts, including the display image and footer. You can also configure the title that appears on user alerts related to protection modules, restrictions, or unknown files.

**STEP 1 |** Create a new agent settings rule.

Select **Settings** > **Agent** > **Settings** and then **Add** a new rule.

**STEP 2 |** *(Optional)* Customize the icon and footer used for all user alert messages.

1. Select **User Alerts** and then select **General Settings (icon and footer).**
2. Customize either or both of the following options:
   - **Icon**—To select an image that will appear in place of the Traps icon in user alert messages, **Browse** to and then **Upload** a new image. The preview on the right allows you to view an example of how the user alert message will look with the new icon.
   - **Action/Footer**—To provide contact or other information along the bottom of the message, enter up to 250 characters. The preview on the right shows your changes as you make them. To specify an email address, use standard HTML format, for example:
     `<a href="mailto://support@organization.com"> Help Desk</a>`
3. Select the Triggering Action: **Prevention Mode** or **Notification Mode**.

**STEP 3 |** *(Optional)* Customize the title text for user alerts.

1. From the **User Alert Window** drop-down, select the type of user alert:
   - **Protection Modules**—A user alert that Traps displays when it activates an exploit or malware protection module to protect a process or block suspicious behavior.
   - **Execution Restrictions**—A user alert that Traps displays when a user opens an executable file from a location that is restricted by a restriction rule.
   - **WildFire Unknowns-Terminate**—A user alert that Traps displays when a user opens an unknown executable file and the WildFire behavior for unknown files is configured to terminate the process
2. Enter the title text to display on the specific user alert type.
3. Select the Triggering Action: **Prevention Mode** or **Notification Mode**.

**STEP 4 |** *(Optional)* Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat to add more conditions as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule.**

**STEP 5 |** *(Optional)* Define the **Target Objects** to which to apply the agent settings rule. By default, a new rule applies to all objects in your organization.
To define a subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 6 | (Optional) Review the rule name and description.** The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 7 | Save the agent settings rule.**

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Settings > Agent > Settings** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Settings** page at any time to **Delete** or **Deactivate** the rule.
Forensics

> Forensics Overview
> Best Practices for Managing Forensic Data
> Manage Forensics Rules and Settings
> Agent Query
Forensics Overview

- Forensics Flow
- Forensic Data Types

Forensics Flow

- Phase 1: Prevention Event Triggered
- Phase 2: Automated Analysis
- Phase 3: Automated Detection
- Phase 4: Collection of Forensic Data

Phase 1: Prevention Event Triggered

When an attacker attempts to exploit a software vulnerability, the Traps protection modules spring into action to halt malicious process behavior and ultimately block the attack. For example, consider the case where a file tries to access crucial DLL metadata from untrusted code locations. If the DLL Security module is enabled to protect processes in your organization, Traps immediately halts the process attempting to access the DLL metadata. Traps records the event in its event log and notifies the user about the security event. If configured, Traps displays a customized notification message (for more information, see Create a Custom User Alert Message).

After successfully halting an exploit attempt, Traps collects and analyzes data related to the event as described in Phase 2: Automated Analysis.

Phase 2: Automated Analysis

When a security event occurs on an endpoint, Traps freezes the contents of the memory, and stores it in a data file known as a memory dump. From the ESM Console you can fine-tune memory dump settings that specify the size of the memory dump—either small, medium, or full (the largest and most complete set of information)—and whether Traps should automatically upload the memory dump to the forensic folder. For more information, see Define Memory Dump Preferences.

After creating the memory dump, Traps deciphers the file and extracts information to identify the underlying cause and to verify the validity of the prevention. Use the results of the analysis to diagnose and understand the event.

Depending on the type of event, Traps may also use automated detection tools to scan for malicious behavior as described in Phase 3: Automated Detection.

Phase 3: Automated Detection

After Traps analyzes the memory dump, Traps automatically performs secondary analysis, the results of which you can use to verify the legitimacy of a prevention event. The secondary analysis provides greater insight into the nature of the event by using detection tools—including ROP chain detection and heap spray detection—to identify additional malicious activity traces.
If the detection tools successfully identify malicious activity traces, Traps stores the information to a system log file on the endpoint using the following syntax: Traps prefix-unique client ID-event ID. Traps also reports the detection to the ESM Server. The ESM Console displays the results in the **Traps Automatic Dump Analysis** section for each prevention event record including whether or not each detection tool was successful in identifying additional malicious activity. If Traps fails to capture the memory, creates the dump file incorrectly, or otherwise fails to complete the secondary analysis, the ESM Console hides this section in the event record.

If the detection tools identify one or more additional malicious activity traces there is a high likelihood that the prevention event is a legitimate threat.

To further troubleshoot or analyze security events, view the forensic data that Traps collects as described in **Phase 4: Collection of Forensic Data**.

**Phase 4: Collection of Forensic Data**

After analyzing the files, Traps notifies the ESM about the security event and can send additional forensic data to the forensic folder.

If your security policy contains a forensic data collection rule, Traps collects one or more specified data types and uploads the file(s) to the forensic folder. Depending on the preferences, Traps can collect URI that were accessed, drivers, files, and relevant DLLs that are loaded in memory under the attacked process, and ancestor processes of the process that triggered the security event. For more information, see **Define Forensics Collection Preferences**.

By default, Traps uses a web-based Background Intelligent Transfer Service (BITS) folder that utilizes idle network bandwidth to upload data. For more information, see **Change the Default Forensic Folder**.

You can also manually retrieve forensic data for a specific security event by creating a one-time action rule to retrieve the data. For more information, see **Retrieve Data About a Security Event**. To view the status of the forensic upload select **Monitor > Data Retrieval**.

**Forensic Data Types**

When a security event occurs on an endpoint, Traps can collect the following information:

<table>
<thead>
<tr>
<th>Forensic Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Dump</td>
<td>Contents of memory locations captured at the time of an event.</td>
</tr>
<tr>
<td>Accessed Files</td>
<td>Files that are loaded in memory under the attacked process for in-depth event inspection including:</td>
</tr>
<tr>
<td></td>
<td>• Relevant DLL retrieval including their path</td>
</tr>
<tr>
<td></td>
<td>• Relevant files from Temporary Internet Files folder</td>
</tr>
<tr>
<td></td>
<td>• Open files (executables and non-executables)</td>
</tr>
<tr>
<td>Loaded Modules</td>
<td>PE image files that are loaded on the system at the time of a security event.</td>
</tr>
<tr>
<td>Accessed URI</td>
<td>Network resources that were accessed at the time of the security event and uniform resource identifier (URI) information.</td>
</tr>
<tr>
<td></td>
<td>The Traps agent can collect accessed URI from Internet Explorer and Firefox browsers only. When an event occurs that is related to other browsers (for example, Microsoft Edge), you will not be able to access URI data for further analysis.</td>
</tr>
<tr>
<td></td>
<td>Collected information includes:</td>
</tr>
<tr>
<td>Forensic Data Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• URIs including hidden links and frames of the relevant attacked threads.</td>
</tr>
<tr>
<td></td>
<td>• Java applet source URIs, filenames and paths, including parents, grandparents, and child processes</td>
</tr>
<tr>
<td></td>
<td>• Collection of URI calls from browser plug-ins, media players, and mail-client software</td>
</tr>
</tbody>
</table>

**Ancestor Processes**

Information about ancestry processes—from browsers, non-browsers, and Java applet child processes—at the time of a security event including:

• Separate sources and destinations for Thread Injection
• Restricted child process parents and grandparents

To customize which types of files are collected, Create a Forensics Rule.
Best Practices for Managing Forensic Data

- **Configure the Forensic Folder to Communicate Over SSL**—To encrypt forensic data, we strongly recommend that you use SSL to communicate with the forensic folder. To use SSL, specify the HTTPS prefix and use port 443 when configuring the Forensic Folder URL (for example, HTTPS://ESMserver.Domain.local:443/BitsUploads).

- **Collect full memory dumps for all processes**—When a security event occurs on the endpoint, Traps can capture the contents of memory related to the protected process and automatically send the data to the ESM Server. This information enables you to further analyze security events when they occur. By sending the full memory dump, Traps captures the most complete amount of data.

- **Create a script to monitor the disk quota**—Due to the lack of an automated deletion mechanism, data related to a large number of prevention events can fill the disk quota on the server that hosts the quarantine folder. As a result, new prevention information will not be written once the quota is full. After the disk quota is full, you cannot erase the prevention data. By creating a script to monitor the disk quota, you can ensure that you are able to monitor and then delete older data, as needed.

- **Enable forensics collection**—When a security event occurs on the endpoint, Traps can collect additional forensic data including which files were accessed, modules that were loaded into memory, URIs that were accessed, and ancestor processes of the process that triggered the security event. You can use the data collected by Traps when troubleshooting a security event. For more information, see Define Forensics Collection Preferences.
Manage Forensics Rules and Settings

- Forensics Rules
- Change the Default Forensic Folder
- Create a Forensics Rule
- Define Memory Dump Preferences
- Define Forensics Collection Preferences
- Retrieve Data About a Security Event

Forensics Rules

*Forensics management rules* enable you to collect forensics data captured by Traps from a central location. From the Policies > Forensics > Management page, you can create rules to manage the following forensics settings:

<table>
<thead>
<tr>
<th>Agent Settings Rules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Memory dump settings</strong></td>
<td>Specify files settings including a size for the memory dump and enable Traps to send the memory dump to the server automatically. This setting only applies to data collected from prevention events related to protected processes. For more information, see Define Memory Dump Preferences.</td>
</tr>
<tr>
<td><strong>Forensics collection</strong></td>
<td>Enable Traps to collect forensic data for each security event including which files were accessed, modules that were loaded into memory, URIs that were accessed, and ancestor processes of the process that triggered the security event. For more information, see Define Forensics Collection Preferences.</td>
</tr>
</tbody>
</table>

Change the Default Forensic Folder

- Change the Forensic Folder Destination Using the ESM Console
- Change the Forensic Folder Destination Using the DB Configuration Tool

**Change the Forensic Folder Destination Using the ESM Console**

To allow you to further troubleshoot or analyze security events, such as a prevention or crash, Traps uploads the forensic data to a web-based forensic folder. During installation of the ESM Console, the installer enables the Background Intelligent Transfer Service (BITS) which utilizes idle network bandwidth to upload the data to forensic folder.

To analyze a security event, create an action rule to retrieve the forensic data from the endpoint (see Manage Data Collected by Traps). When Traps receives the request to send the data, it copies the files to the forensic folder (also referred to in the Endpoint Security Manager as the quarantine folder), which is a local or network path that you specify during the initial installation.

You can change the path of the forensic folder at any time using the Endpoint Security Manager or using the DB Configuration Tool (see Change the Forensic Folder Destination Using the DB Configuration Tool). All endpoints must have write-permission to this folder.

**STEP 1| Select Settings > ESM > Settings.**
STEP 2 | In the Server Configuration area, enter the web-based URL, in the **Forensic Folder URL** field to use BITS to upload forensic data.

*To encrypt forensic data, we strongly recommend that you use SSL to communicate with the forensic folder. To use SSL, include the fully qualified domain name (FQDN) and specify port 443, for example **HTTPS://ESMserver.Domain.local:443/BitsUploads**. If you are not using SSL, specify port 80, for example **http://ESMSERVER:80/BitsUploads**.*

**Change the Forensic Folder Destination Using the DB Configuration Tool**

To allow you to further troubleshoot or analyze security events, such as a prevention or crash, Traps uploads the forensic data to a web-based forensic folder. During installation of the ESM Console, the installer enables the Background Intelligent Transfer Service (BITS) which utilizes idle network bandwidth to upload the data to forensic folder.

To analyze a security event, create an action rule to retrieve the forensic data from the endpoint (see Manage Data Collected by Traps). When Traps receives the request to send the data, it copies the files to the forensic folder (also referred to in the Endpoint Security Manager as the quarantine folder), which is a local or network path that you specify during the initial installation.

You can change the path of the forensic folder at any time using the Endpoint Security Manager (see Change the Forensic Folder Destination Using the ESM Console) or using the Database (DB) Configuration Tool.

The DB Configuration Tool is a command-line interface that provides an alternative to managing basic server settings using the ESM Console. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt run as an administrator. The DB Configuration Tool is located in the Server folder on the ESM Server.

*All commands run using the DB Configuration Tool are case sensitive.*

**STEP 1 |** Open a command prompt as an administrator:

- Select **Start > All Programs > Accessories.** Right-click **Command prompt**, and then select **Run as administrator**.
- Select **Start.** In the **Start Search** box, type **cmd.** Then, to open the command prompt as an administrator, press **CTRL+SHIFT+ENTER.**

**STEP 2 |** Navigate to the folder that contains the DB Configuration Tool:

```
C:\Users\Administrator> cd
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server
```

**STEP 3 |** *(Optional)* View the existing server settings:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server show
PreventionsDestFolder = \\ESMServer\Quarantine
InventoryInterval = 284
HeartBeatGracePeriod = 4200
NinjaModePassword = Password2
BitsUrl = https://CYVERASERVER.Domain.local:443/BitsUploads
```
MaxActions = 5000

**STEP 4 |** Enter the web-based URL of the forensics folder.

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server BitsUrl http://ESMserver.Domain.local:443/BitsUploads
```

To encrypt forensic data, we strongly recommend that you use SSL to communicate with the forensic folder. To use SSL, include the fully qualified domain name (FQDN) and specify port 443, for example HTTPS://ESMserver.Domain.local:443/BitsUploads. If you are not using SSL, specify port 80, for example http://ESMserver:80/BitsUploads.

**STEP 5 |** *(Optional)* To verify the path of the forensic folder, run the `dbconfig server show` command:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server show
PreventionsDestFolder = \\ESMServer-New\Quarantine
InventoryInterval = 284
HeartBeatGracePeriod = 4200
NinjaModePassword = Password2
BitsUrl = HTTPS://ESMserver.Domain.local:443/BitsUploads
MaxActions = 5000
```

Create a Forensics Rule

Create a forensics rule to define memory dump and forensics collection preferences.

**STEP 1 |** Configure a new forensics rule.

Select Policies > Forensics > Management and then click Add.

**STEP 2 |** Select the type of rule you want to configure.

Select one of the following types of forensics rules and configure the settings according to the type of rule:

- **Memory Dump**—For more information, see Define Memory Dump Preferences.
- **Forensics Collection**—For more information, see Define Forensics Collection Preferences.

**STEP 3 |** *(Optional)* Add Conditions to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the Conditions tab, select the condition in the Conditions list, and then Add it to the Selected Conditions list. Repeat to add more conditions, as needed. To add a condition to the Conditions list, see Define Activation Conditions for a Rule.

**STEP 4 |** *(Optional)* Define the Target Objects to which to apply the restriction rule.

To define a smaller subset of target objects, select the Objects tab, and then enter one or more Users, Computers, Groups, Organizational Unit, or Existing Endpoints in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.
STEP 5 | *(Optional)* Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

STEP 6 | **Save the forensics rule.**

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Policies > Forensics > Management** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Management** page at any time to **Delete** or **Deactivate** the rule.

**Define Memory Dump Preferences**

When a protected process crashes or terminates abnormally, Traps records information about the event including the contents of memory locations and other data about the event in what is known as a memory dump.

Create a forensics rule to determine how Traps manages process-related memory dumps including whether to send memory dumps automatically to the forensic folder or change the size of the memory dump, either small, medium, or full (the largest and most complete set of information).

STEP 1 | **Configure a new forensics rule.**

Select **Policies > Forensics > Management** and then click **Add**.

STEP 2 | **Define memory dump preferences when a prevention event occurs on the endpoint.**

1. Select **Memory Dump** and then select either of the following preferences:
   - Automatically send the memory dumps to the server by selecting **Send the memory dumps automatically**.
   - Specify the size of the memory dump file by selecting the **Memory dump size** option and then selecting **Small**, **Medium**, or **Full** from the drop-down.

2. Select the source processes from with Traps will collect memory dumps, either one or more **Specific processes** or **All processes**.

STEP 3 | *(Optional)* **Add Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat to add more conditions, as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

STEP 4 | *(Optional)* Define the **Target Objects** to which to apply the restriction rule.

To define a smaller subset of target objects, select the **Objects** tab, and then enter one or more **Users**, **Computers**, **Groups**, **Organizational Unit**, or **Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.
STEP 5 | **Optional** Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

STEP 6 | **Save** the forensics rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Policies > Forensics > Management** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Management** page at any time to **Delete** or **Deactivate** the rule.

**Define Forensics Collection Preferences**

To help you better understand and derive implications about the true nature of a security event when it occurs on an endpoint, you can configure forensics collection options. At the time of a security event, Traps can report the files that were accessed, modules that were loaded into memory, URIs that were accessed, and ancestor processes of the process that triggered the security event.

STEP 1 | **Configure** a new forensics rule.

Select **Policies > Forensics > Management** and then click **Add**.

STEP 2 | **Define** forensics collection preferences.

Select **Forensics Collection** and then configure preferences in the following fields:

- **Report Accessed Files**—Select **Enabled** to collect information about files that are loaded in memory under the attacked process for in-depth event inspection.
- **Report Loaded Modules**—Select **Enabled** to report which PE image files are loaded on the system at the time of a security event.
- **Report Accessed URI**—Select **Enabled** to collect network resources that were accessed at the time of the security event and uniform resource identifier (URI) information from web plug-ins, media players, and mail clients.
- **Report Ancestor Processes**—Some applications can run Java applets as a process child, and even as a process child of a process child and so on. Select **Enabled** to record information about the ancestry processes from browsers, non-browsers, and Java applet child processes to allow you to better understand the root of an event.

Alternatively, for each data type, you can **Disable** forensics collection or **Inherit** the settings from the default security policy.

STEP 3 | **Optional** Add **Conditions** to the rule. By default, a new rule does not contain any conditions.

To specify a condition, select the **Conditions** tab, select the condition in the Conditions list, and then **Add** it to the Selected Conditions list. Repeat to add more conditions, as needed. To add a condition to the Conditions list, see **Define Activation Conditions for a Rule**.

STEP 4 | **Optional** Define the **Target Objects** to which to apply the forensics rule. By default, a new rule applies to all objects in your organization. To define a smaller subset of target objects,
To define a smaller subset of target objects, select the **Objects** tab, and then enter one or more **Users, Computers, Groups, Organizational Unit, or Existing Endpoints** in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

**STEP 5** | *(Optional)* Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the **Name** tab, clear the **Activate automatic description** option, and then enter a rule name and description of your choice.

**STEP 6** | Save the forensics rule.

Do either of the following:

- **Save** the rule without activating it. This option is only available for inactive, cloned, or new rules. When you are ready to activate the rule, select the rule from the **Policies > Forensics > Management** page and then click **Activate**.
- **Apply** the rule to activate it immediately.

After saving or applying a rule, you can return to the **Management** page at any time to **Delete** or **Deactivate** the rule.

**Retrieve Data About a Security Event**

When a security event occurs on an endpoint, Traps collects forensic data including the contents of memory and stores it on the endpoint. Use the forensic data to debug an issue or investigate a specific problem with an application. Selecting this option creates an agent settings rule to retrieve the information collected by Traps. After Traps receives the agent settings rule, the agent sends all the logs to the designated forensic folder.

To create a general rule to retrieve data from one or more endpoints, see **Manage Data Collected by Traps**.

**STEP 1** | From the ESM Console, select **Security Events > Threats** to view security events related to protected processes, or **Monitor > Provisional Mode** to view security events related to provisional processes.

**STEP 2** | Select the security event for which you want to retrieve data. The event expands to display further details and actions about the security event.
STEP 3 | Click **Retrieve Data**. The ESM Console populates the settings for an agent settings rule.

STEP 4 | Review the rule details, and then click **Apply** to activate the rule immediately or **Save** to activate the rule at a later date. At the next heartbeat communication with the ESM Server, the Traps agent receives the new rule and sends the prevention data to the forensics folder.

STEP 5 | To view the status of the forensic upload select **Monitor > Data Retrieval**.

STEP 6 | After the upload is complete, click **Download** to save the prevention data locally or navigate to the forensic folder. If you are no longer require the prevention data, you can, optionally, **Delete** it from the Data Retrieval table.
Agent Query

Use the Agent Query to search your endpoints for a system file, folder, or registry key. Each query runs in real-time as a one-time action rule and enables you to search for multiple parameters from a central location.

- Agent Query Flow
- Search Endpoints for a File, Folder, or Registry Key
- View the Results of an Agent Query

Agent Query Flow

After you create an agent query to Search Endpoints for a File, Folder, or Registry Key, the ESM Server sends the query in the form of a one-time action rule at the next heartbeat communication with the agent. If the query contains target objects and/or conditions, the ESM Server sends the query to only those endpoints that match the target objects and conditions. If you did not specify any target objects or conditions, the ESM Server sends the query to all endpoints.

When the Traps agent receives the query, it immediately searches the endpoint for the filename, folder, and/or registry key on the local endpoint. If the query contains multiple search parameters, Traps evaluates the queries separately and reports a match if it finds any of the search criteria. In the case of a matching system file, the Traps agent also captures metadata about the file. The Traps agent then sends the information to the ESM Server at the next heartbeat communication.

To see the latest search results, refresh the Agent Query page at any time. The ESM Console displays up to 50 results in the Details view of each search query (see View the Results of an Agent Query).

Search Endpoints for a File, Folder, or Registry Key

To perform a centralized search for a system file, folder, or registry key, use the Agent Query.

STEP 1 | Create a new query.
1. From the ESM Console, select Policies > Forensics > Agent Query.
2. Add a new query.

STEP 2 | Configure one or more search parameters for the query. When multiple search parameters are specified, Traps will return a result if the search matches any of the parameters.
1. Select the search parameters, either a File name, Folder name, or Registry Key name.
2. Enter the matching search value, and then click Add.

Optionally, you can use wildcards in the last portion of the file or folder name path, for example: C:\Temp\*.txt
3. Repeat as needed to enter multiple search criteria.

STEP 3 | (Optional) Add conditions to the query.

Conditions specified here can restrict the scope of the query by sending it to only endpoints that match or do not match the condition.

1. From the Conditions tab, select the condition in the Conditions list and click Add next to the appropriate include or exclude condition list.
2. Repeat to add more conditions, if desired.
STEP 4 | (Optional) Define the target objects to which to apply the query. By default, the ESM server sends the query to all endpoints in your organization.

Like conditions, target objects can decrease the scope of a query by targeting specific Users, Computers, Groups, Organizational Unit, or Existing Endpoints.

Select the Objects tab, and then enter one or more target objects in the Include or Exclude areas. The Endpoint Security Manager queries Active Directory to verify the users, computers, groups, or organizational units or identifies existing endpoints from previous communication messages.

STEP 5 | (Optional) Review the rule name and description. The ESM Console automatically generates the rule name and description based on the rule details but permits you to change these fields, if needed.

To override the autogenerated name, select the Name tab, clear the Activate automatic description option, and then enter a rule name and description of your choice.

STEP 6 | Save the query.

Do either of the following:
- Save the query without activating it. When you are ready to run the query, select the rule from the Policies > Forensics > Agent Query page and then click Activate.
- Apply the query to run it immediately.

STEP 7 | Review the results of the query.

Although the Agent Query searches in real-time, the ESM Console does not automatically refresh the page with the query results. As a result, you must refresh the page to view the current results.

See View the Results of an Agent Query.

View the Results of an Agent Query

The Agent Query page displays all saved and applied queries and enables you to review results for applied queries. By expanding the row for the query, you can view additional information about matches including when and on which computer the match was found, the file or registry key that matched the search parameter, and metadata details for the file. Use the results you receive after you run an agent query to identify and take additional action, if needed, to secure the endpoint.

STEP 1 | From the Policies > Forensics > Agent Query page, select the row for the applied query. The row expands to display additional information about the query and includes any matches for the query in the Agent Query, Found matches section.

For each applied query, the ESM Console displays the number of endpoints that received the query (Applied On), the number of endpoints which successfully executed the search (Succeeded), and the number of endpoints which failed to run the query or did not receive the query (Failed).

STEP 2 | (Optional) To view detailed information about the match, click Details.

The ESM Console displays up to 50 records of matches.

STEP 3 | (Optional) To view the full text, hover over cell of the Result or Metadata field.

STEP 4 | (Optional) To save the results to a comma-separated (CSV) file that you can parse, click the action menu at the top of the page and select Export Logs.
STEP 5 | (Optional) There are additional tasks you can perform after reviewing the results of the query:

- RemEDIATE any issues with malicious files on the endpoint.
- **Duplicate** the query, make any changes as required, and **Apply** it to run it again.
- **Delete** the query and results from the ESM Console.
Reports and Logging

The Endpoint Security Manager can write logs to an external logging platform, such as security information and event management (SIEM), Service Organization Controls (SOCs), or syslog, in addition to storing its logs internally. The Endpoint Security Manager can also send logs to an email address. Specifying an external logging platform allows an aggregated view of logs from all ESM components.

- Event Log Types
- Common Variables Used in Events
- Forward Logs to an External Logging Platform
- Forward Logs to Email
Event Log Types

The ESM Console displays information about events that occur on your Traps components on the Logs and Security Events pages. The events can include security events, policy changes, agent and ESM Server status changes, and changes to settings. When you enable log forwarding to a SIEM or syslog device, or to an email, you can customize the type of events that the ESM Console sends. The events are grouped into the following categories based on the type of event:

- Security Events
- Policies - General
- Policies - Rules
- Policies - Process Management
- Policies - Restriction Settings
- Policies - Hash Control
- Monitor - Agent
- Monitor ESM
- Settings - Administration
- Settings - Agent
- Settings - ESM
- Settings - Conditions
- Settings - Licenses

Security Events

The following table displays the security event logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention Event</td>
<td>A process or executable file was blocked.</td>
</tr>
<tr>
<td></td>
<td>• CEF—PreventionEvent</td>
</tr>
<tr>
<td></td>
<td>• LEEF—PreventionEvent</td>
</tr>
<tr>
<td></td>
<td>• Syslog—PreventionEvent</td>
</tr>
<tr>
<td></td>
<td>• Email—PreventionEvent</td>
</tr>
<tr>
<td>Notification Event</td>
<td>A process or executable file exhibited suspicious behavior.</td>
</tr>
<tr>
<td></td>
<td>• CEF—NotificationEvent</td>
</tr>
<tr>
<td></td>
<td>• LEEF—NotificationEvent</td>
</tr>
<tr>
<td></td>
<td>• Syslog—NotificationEvent</td>
</tr>
<tr>
<td></td>
<td>• Email—NotificationEvent</td>
</tr>
<tr>
<td>Provisional Event</td>
<td>A provisional process exhibited suspicious behavior.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ProvisionalEvent</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ProvisionalEvent</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ProvisionalEvent</td>
</tr>
<tr>
<td></td>
<td>• Email—ProvisionalEvent</td>
</tr>
</tbody>
</table>
### Post Detection Event
An executable file that was previously allowed to run on an endpoint was determined to be malware. Post detection events provide notifications for each endpoint on which the file executed.

- CEF—*PostDetectionEvent*
- LEEF—*PostDetectionEvent*
- Syslog—*PostDetectionEvent*
- Email—*PostDetectionEvent*

### Policies - General

The following table displays the general policy logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Disabled</td>
<td>An administrator disabled protection of all security rules on the ESM Console.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>DisabledProtection</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>DisabledProtection</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>DisabledProtection</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>DisabledProtection</em></td>
</tr>
<tr>
<td>Protection Enabled</td>
<td>An administrator re-enabled protection by all security rules on the ESM Console.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>EnabledProtection</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>EnabledProtection</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>EnabledProtection</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>EnabledProtection</em></td>
</tr>
<tr>
<td>Server Content Update Success</td>
<td>A content update was installed.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>ServerContentUpdateSuccess</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>ServerContentUpdateSuccess</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>ServerContentUpdateSuccess</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>ServerContentUpdateSuccess</em></td>
</tr>
<tr>
<td>Server Content Update Failure</td>
<td>A content update failed to install.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>ServerContentUpdateFailure</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>ServerContentUpdateFailure</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>ServerContentUpdateFailure</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>ServerContentUpdateFailure</em></td>
</tr>
<tr>
<td>Server Content Revert Success</td>
<td>A content update was rolled back to an older version.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>ServerContentRevertSuccess</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>ServerContentRevertSuccess</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>ServerContentRevertSuccess</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>ServerContentRevertSuccess</em></td>
</tr>
</tbody>
</table>
### Server Content Revert Failure

A content update failed to roll back to an older version.
- **CEF**—ServerContentRevertFailure
- **LEEF**—ServerContentRevertFailure
- **Syslog**—ServerContentRevertFailure
- **Email**—ServerContentRevertFailure

### Policies - Rules

The following table displays the policy rule logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Added/Edited</td>
<td>An administrator added a new rule or edited an existing rule.</td>
</tr>
<tr>
<td></td>
<td>• CEF—RuleEdited</td>
</tr>
<tr>
<td></td>
<td>• LEEF—RuleEdited</td>
</tr>
<tr>
<td></td>
<td>• Syslog—RuleEdited</td>
</tr>
<tr>
<td></td>
<td>• Email—RuleEdited</td>
</tr>
<tr>
<td>Rule Deleted</td>
<td>An administrator deleted a rule.</td>
</tr>
<tr>
<td></td>
<td>• CEF—RuleDeleted</td>
</tr>
<tr>
<td></td>
<td>• LEEF—RuleDeleted</td>
</tr>
<tr>
<td></td>
<td>• Syslog—RuleDeleted</td>
</tr>
<tr>
<td></td>
<td>• Email—RuleDeleted</td>
</tr>
</tbody>
</table>

### Policies - Process Management

The following table displays the process management logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Added/Edited</td>
<td>An administrator added or edited a process.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ProcessEdited</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ProcessEdited</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ProcessEdited</td>
</tr>
<tr>
<td></td>
<td>• Email—ProcessEdited</td>
</tr>
<tr>
<td>Process Deleted</td>
<td>An administrator added or edited a process.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ProcessDeleted</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ProcessDeleted</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ProcessDeleted</td>
</tr>
<tr>
<td></td>
<td>• Email—ProcessDeleted</td>
</tr>
</tbody>
</table>
Policies - Restriction Settings

The following table displays the restriction settings logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restriction Settings Add/Edit</td>
<td>An administrator added or edited a global restriction setting.</td>
</tr>
<tr>
<td></td>
<td>• CEF—RestrictionSettingsEdited</td>
</tr>
<tr>
<td></td>
<td>• LEEF—RestrictionSettingsEdited</td>
</tr>
<tr>
<td></td>
<td>• Syslog—RestrictionSettingsEdited</td>
</tr>
<tr>
<td></td>
<td>• Email—RestrictionSettingsEdited</td>
</tr>
</tbody>
</table>

Policies - Hash Control

The following table displays the hash control logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Added</td>
<td>A hash was added to the ESM Server cache.</td>
</tr>
<tr>
<td></td>
<td>• CEF—NewHash</td>
</tr>
<tr>
<td></td>
<td>• LEEF—NewHash</td>
</tr>
<tr>
<td></td>
<td>• Syslog—NewHash</td>
</tr>
<tr>
<td></td>
<td>• Email—NewHash</td>
</tr>
<tr>
<td>Verdict Changed - Any to Any</td>
<td>A hash verdict has changed to malicious.</td>
</tr>
<tr>
<td></td>
<td>• CEF—VerdictChange</td>
</tr>
<tr>
<td></td>
<td>• LEEF—VerdictChange</td>
</tr>
<tr>
<td></td>
<td>• Syslog—VerdictChange</td>
</tr>
<tr>
<td></td>
<td>• Email—VerdictChange</td>
</tr>
<tr>
<td>Verdict Changed - Any to Malware</td>
<td>A hash verdict has changed to malicious.</td>
</tr>
<tr>
<td></td>
<td>• CEF—VerdictChangeAnyToMalware</td>
</tr>
<tr>
<td></td>
<td>• LEEF—VerdictChangeAnyToMalware</td>
</tr>
<tr>
<td></td>
<td>• Syslog—VerdictChangeAnyToMalware</td>
</tr>
<tr>
<td></td>
<td>• Email—VerdictChangeAnyToMalware</td>
</tr>
<tr>
<td>Verdict Changed - Malware to Any</td>
<td>The verdict of a hash has changed from malicious to a new verdict.</td>
</tr>
<tr>
<td></td>
<td>• CEF—VerdictChangeMalwareToAny</td>
</tr>
<tr>
<td></td>
<td>• LEEF—VerdictChangeMalwareToAny</td>
</tr>
<tr>
<td></td>
<td>• Syslog—VerdictChangeMalwareToAny</td>
</tr>
<tr>
<td></td>
<td>• Email—VerdictChangeMalwareToAny</td>
</tr>
<tr>
<td>Verdict Changed - No connection to Any</td>
<td>The verdict of a hash has changed from no connection to a new verdict.</td>
</tr>
<tr>
<td></td>
<td>• CEF—VerdictChangeNoConnectionToAny</td>
</tr>
<tr>
<td></td>
<td>• LEEF—VerdictChangeNoConnectionToAny</td>
</tr>
<tr>
<td></td>
<td>• Syslog—VerdictChangeNoConnectionToAny</td>
</tr>
</tbody>
</table>
### Event Name

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verdict Changed - Unknown to Any</strong></td>
<td>The verdict of a hash has changed from unknown to a new verdict.</td>
</tr>
<tr>
<td>• Email—VerdictChangeUnknownToAny</td>
<td></td>
</tr>
<tr>
<td>• CEF—VerdictChangeUnknownToAny</td>
<td></td>
</tr>
<tr>
<td>• LEEF—VerdictChangeUnknownToAny</td>
<td></td>
</tr>
<tr>
<td>• Syslog—VerdictChangeUnknownToAny</td>
<td></td>
</tr>
<tr>
<td>• Email—VerdictChangeUnknownToAny</td>
<td></td>
</tr>
<tr>
<td><strong>Hashes Imported</strong></td>
<td>An administrator has imported one or more hashes into the server cache.</td>
</tr>
<tr>
<td>• CEF—HashesImport</td>
<td></td>
</tr>
<tr>
<td>• LEEF—HashesImport</td>
<td></td>
</tr>
<tr>
<td>• Syslog—HashesImport</td>
<td></td>
</tr>
<tr>
<td>• Email—HashesImport</td>
<td></td>
</tr>
<tr>
<td><strong>Verdict Changed - Manual Override</strong></td>
<td>An administrator manually set a verdict for hash.</td>
</tr>
<tr>
<td>• CEF—VerdictManualOverride</td>
<td></td>
</tr>
<tr>
<td>• LEEF—VerdictManualOverride</td>
<td></td>
</tr>
<tr>
<td>• Syslog—VerdictManualOverride</td>
<td></td>
</tr>
<tr>
<td>• Email—VerdictManualOverride</td>
<td></td>
</tr>
<tr>
<td><strong>Verdict Changed - Reverted To WildFire</strong></td>
<td>An administrator removed a manual override for a hash and reverted to the last known WildFire verdict.</td>
</tr>
<tr>
<td>• CEF—VerdictRevertedToWildfire</td>
<td></td>
</tr>
<tr>
<td>• LEEF—VerdictRevertedToWildfire</td>
<td></td>
</tr>
<tr>
<td>• Syslog—VerdictRevertedToWildfire</td>
<td></td>
</tr>
<tr>
<td>• Email—VerdictRevertedToWildfire</td>
<td></td>
</tr>
</tbody>
</table>

### Monitor - Agent

The following table displays the agent logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Access Violation</strong></td>
<td>An agent reported an access violation.</td>
</tr>
<tr>
<td>• CEF—AccessViolation</td>
<td></td>
</tr>
<tr>
<td>• LEEF—AccessViolation</td>
<td></td>
</tr>
<tr>
<td>• Syslog—AccessViolation</td>
<td></td>
</tr>
<tr>
<td>• Email—AccessViolation</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Heartbeat - Any</strong></td>
<td>A heartbeat was received from the agent.</td>
</tr>
<tr>
<td>• CEF—Heartbeat</td>
<td></td>
</tr>
<tr>
<td>• LEEF—Heartbeat</td>
<td></td>
</tr>
<tr>
<td>• Syslog—Heartbeat</td>
<td></td>
</tr>
<tr>
<td>• Email—Heartbeat</td>
<td></td>
</tr>
<tr>
<td>Event Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Agent Service Start</td>
<td>The agent service was started on the endpoint.</td>
</tr>
<tr>
<td>Agent Service Stopped</td>
<td>The agent service was stopped on the endpoint.</td>
</tr>
<tr>
<td>Agent Shutdown</td>
<td>The endpoint was shut down.</td>
</tr>
<tr>
<td>Agent Service Start Failed</td>
<td>The agent service failed to start on the endpoint.</td>
</tr>
<tr>
<td>Agent Service Warning</td>
<td>The agent service reported a warning.</td>
</tr>
<tr>
<td>Process Crash</td>
<td>A process has crashed on the endpoint.</td>
</tr>
<tr>
<td>Agent Process Injection</td>
<td>The agent exceeded the permissible amount of time to inject into a process.</td>
</tr>
<tr>
<td>Agent Reporting Service</td>
<td>The agent reporting service failed to start.</td>
</tr>
<tr>
<td>Event Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• <strong>Agent File Upload Failed</strong></td>
<td>The agent failed to upload a file.</td>
</tr>
<tr>
<td>• CEF—FileUploadFailure</td>
<td></td>
</tr>
<tr>
<td>• LEEF—FileUploadFailure</td>
<td></td>
</tr>
<tr>
<td>• Syslog—FileUploadFailure</td>
<td></td>
</tr>
<tr>
<td>• Email—FileUploadFailure</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Installed to System</strong></td>
<td>Traps was installed on an endpoint.</td>
</tr>
<tr>
<td>• CEF—ClientInstall</td>
<td></td>
</tr>
<tr>
<td>• LEEF—ClientInstall</td>
<td></td>
</tr>
<tr>
<td>• Syslog—ClientInstall</td>
<td></td>
</tr>
<tr>
<td>• Email—ClientInstall</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Uninstalled from System</strong></td>
<td>Traps was uninstalled from an endpoint.</td>
</tr>
<tr>
<td>• CEF—ClientUninstall</td>
<td></td>
</tr>
<tr>
<td>• LEEF—ClientUninstall</td>
<td></td>
</tr>
<tr>
<td>• Syslog—ClientUninstall</td>
<td></td>
</tr>
<tr>
<td>• Email—ClientUninstall</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Upgraded</strong></td>
<td>Traps was upgraded on an endpoint.</td>
</tr>
<tr>
<td>• CEF—ClientUpgrade</td>
<td></td>
</tr>
<tr>
<td>• LEEF—ClientUpgrade</td>
<td></td>
</tr>
<tr>
<td>• Syslog—ClientUpgrade</td>
<td></td>
</tr>
<tr>
<td>• Email—ClientUpgrade</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Status Change</strong></td>
<td>The agent status has changed.</td>
</tr>
<tr>
<td>• CEF—TrapsServiceStatusChange</td>
<td></td>
</tr>
<tr>
<td>• LEEF—TrapsServiceStatusChange</td>
<td></td>
</tr>
<tr>
<td>• Syslog—TrapsServiceStatusChange</td>
<td></td>
</tr>
<tr>
<td>• Email—TrapsServiceStatusChange</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Policy Change</strong></td>
<td>The agent policy has changed.</td>
</tr>
<tr>
<td>• CEF—AgentPolicyChange</td>
<td></td>
</tr>
<tr>
<td>• LEEF—AgentPolicyChange</td>
<td></td>
</tr>
<tr>
<td>• Syslog—AgentPolicyChange</td>
<td></td>
</tr>
<tr>
<td>• Email—AgentPolicyChange</td>
<td></td>
</tr>
<tr>
<td><strong>Local Analysis Feature Extraction Failed</strong></td>
<td>The file that local analysis tried to examine was corrupt and could not be examined using local analysis. When this occurs, Traps identifies the file as malware until it receives a verdict (either from WildFire or the administrative hash control policy).</td>
</tr>
<tr>
<td>• CEF—LocalAnalysisFeatureExtractionFailed</td>
<td></td>
</tr>
<tr>
<td>• LEEF—LocalAnalysisFeatureExtractionFailed</td>
<td></td>
</tr>
<tr>
<td>• Syslog—LocalAnalysisFeatureExtractionFailed</td>
<td></td>
</tr>
<tr>
<td>Event Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Analysis Model</td>
<td>The local analysis model was missing on the endpoint and was therefore</td>
</tr>
<tr>
<td>Unavailable</td>
<td>disabled.</td>
</tr>
<tr>
<td></td>
<td>• CEF—LocalAnalysisModelUnavailable</td>
</tr>
<tr>
<td></td>
<td>• LEEF—LocalAnalysisModelUnavailable</td>
</tr>
<tr>
<td></td>
<td>• Syslog—LocalAnalysisModelUnavailable</td>
</tr>
<tr>
<td></td>
<td>• Email—LocalAnalysisModelUnavailable</td>
</tr>
<tr>
<td>Local Analysis Module</td>
<td>The local analysis model successfully analyzed an unknown executable file</td>
</tr>
<tr>
<td>Succeeded</td>
<td>and issued a verdict.</td>
</tr>
<tr>
<td></td>
<td>• CEF—LocalAnalysisModuleSucceeded</td>
</tr>
<tr>
<td></td>
<td>• LEEF—LocalAnalysisModuleSucceeded</td>
</tr>
<tr>
<td></td>
<td>• Syslog—LocalAnalysisModuleSucceeded</td>
</tr>
<tr>
<td></td>
<td>• Email—LocalAnalysisModuleSucceeded</td>
</tr>
<tr>
<td>Local Analysis Module</td>
<td>The local analysis model failed to analyze an unknown executable file and</td>
</tr>
<tr>
<td>Failed</td>
<td>issue a verdict.</td>
</tr>
<tr>
<td></td>
<td>• CEF—LocalAnalysisModuleFailed</td>
</tr>
<tr>
<td></td>
<td>• LEEF—LocalAnalysisModuleFailed</td>
</tr>
<tr>
<td></td>
<td>• Syslog—LocalAnalysisModuleFailed</td>
</tr>
<tr>
<td></td>
<td>• Email—LocalAnalysisModuleFailed</td>
</tr>
<tr>
<td>Trusted Signer Changed</td>
<td>The local decision of a trusted signer on the agent has changed. This can</td>
</tr>
<tr>
<td></td>
<td>be due a change in the local certificate store on the endpoint, a content</td>
</tr>
<tr>
<td></td>
<td>update containing changes to the trusted signer list, or a manual update to</td>
</tr>
<tr>
<td></td>
<td>the trusted signers list.</td>
</tr>
<tr>
<td></td>
<td>• CEF—PublisherChanged</td>
</tr>
<tr>
<td></td>
<td>• LEEF—PublisherChanged</td>
</tr>
<tr>
<td></td>
<td>• Syslog—PublisherChanged</td>
</tr>
<tr>
<td></td>
<td>• Email—PublisherChanged</td>
</tr>
<tr>
<td>Agent Content Update</td>
<td>The agent received a new content update version.</td>
</tr>
<tr>
<td></td>
<td>• CEF—AgentContentUpdate</td>
</tr>
<tr>
<td></td>
<td>• LEEF—AgentContentUpdate</td>
</tr>
<tr>
<td></td>
<td>• Syslog—AgentContentUpdate</td>
</tr>
<tr>
<td></td>
<td>• Email—AgentContentUpdate</td>
</tr>
<tr>
<td>Quarantine Quota Exceeded</td>
<td>The storage quota for quarantined files on the endpoint has been exceeded.</td>
</tr>
<tr>
<td></td>
<td>• CEF—QuarantineQuotaExceeded</td>
</tr>
<tr>
<td></td>
<td>• LEEF—QuarantineQuotaExceeded</td>
</tr>
<tr>
<td></td>
<td>• Syslog—QuarantineQuotaExceeded</td>
</tr>
<tr>
<td></td>
<td>• Email—QuarantineQuotaExceeded</td>
</tr>
</tbody>
</table>
Monitor ESM

The following table displays the ESM logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login</td>
<td>An administrator has logged in to the ESM Console.</td>
</tr>
<tr>
<td></td>
<td>• CEF—UserLogin</td>
</tr>
<tr>
<td></td>
<td>• LEEF—UserLogin</td>
</tr>
<tr>
<td></td>
<td>• Syslog—UserLogin</td>
</tr>
<tr>
<td></td>
<td>• Email—UserLogin</td>
</tr>
<tr>
<td>ESM Heartbeat</td>
<td>A heartbeat was received from the ESM Server.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ServerHeartbeat</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ServerHeartbeat</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ServerHeartbeat</td>
</tr>
<tr>
<td></td>
<td>• Email—ServerHeartbeat</td>
</tr>
<tr>
<td>ESM Configuration Changed</td>
<td>The ESM Server configuration was changed.</td>
</tr>
<tr>
<td></td>
<td>• CEF—EsmConfigurationChange</td>
</tr>
<tr>
<td></td>
<td>• LEEF—EsmConfigurationChange</td>
</tr>
<tr>
<td></td>
<td>• Syslog—EsmConfigurationChange</td>
</tr>
<tr>
<td></td>
<td>• Email—EsmConfigurationChange</td>
</tr>
<tr>
<td>ESM Status Changed</td>
<td>The status of the ESM Server has changed.</td>
</tr>
<tr>
<td></td>
<td>• CEF—EsmStatusChange</td>
</tr>
<tr>
<td></td>
<td>• LEEF—EsmStatusChange</td>
</tr>
<tr>
<td></td>
<td>• Syslog—EsmStatusChange</td>
</tr>
<tr>
<td></td>
<td>• Email—EsmStatusChange</td>
</tr>
<tr>
<td>Tech Support File Status</td>
<td>The status of the ESM tech support file has changed.</td>
</tr>
<tr>
<td></td>
<td>• CEF—TechSupportFileStatus</td>
</tr>
<tr>
<td></td>
<td>• LEEF—TechSupportFileStatus</td>
</tr>
<tr>
<td></td>
<td>• Syslog—TechSupportFileStatus</td>
</tr>
<tr>
<td></td>
<td>• Email—TechSupportFileStatus</td>
</tr>
<tr>
<td>Communication Check with Proxy</td>
<td>A proxy communication event occurred between the ESM components and the</td>
</tr>
<tr>
<td></td>
<td>proxy server. Proxy communication events can disrupt communication with</td>
</tr>
<tr>
<td></td>
<td>WildFire.</td>
</tr>
<tr>
<td></td>
<td>• CEF—CommunicationsCheckWithProxy</td>
</tr>
<tr>
<td></td>
<td>• LEEF—CommunicationsCheckWithProxy</td>
</tr>
<tr>
<td></td>
<td>• Syslog—CommunicationsCheckWithProxy</td>
</tr>
<tr>
<td></td>
<td>• Email—CommunicationsCheckWithProxy</td>
</tr>
<tr>
<td>WildFire Communication Status</td>
<td>The communication status between the ESM Server and WildFire has changed</td>
</tr>
<tr>
<td>Changed</td>
<td>from reachable to unreachable or from unreachable to reachable.</td>
</tr>
<tr>
<td></td>
<td>• CEF—WfCommunicationsStatusChanged</td>
</tr>
<tr>
<td></td>
<td>• LEEF—WfCommunicationsStatusChanged</td>
</tr>
</tbody>
</table>
### Event Name | Description
---|---
Role Deleted | An administrative role was deleted.
- **CEF**—RoleDeleted
- **LEEF**—RoleDeleted
- **Syslog**—RoleDeleted
- **Email**—RoleDeleted

Role Added/Edited | An administrative role was added or edited.
- **CEF**—RoleEdited
- **LEEF**—RoleEdited
- **Syslog**—RoleEdited
- **Email**—RoleEdited

Role Status Changed | The status of an administrative role was changed.
- **CEF**—RoleStatusChanged
- **LEEF**—RoleStatusChanged
- **Syslog**—RoleStatusChanged
- **Email**—RoleStatusChanged

User Deleted | An administrative user was deleted.
- **CEF**—UserDeleted
- **LEEF**—UserDeleted
- **Syslog**—UserDeleted
- **Email**—UserDeleted

User Added/Edited | An administrative user was added or deleted.
- **CEF**—UserEdited
- **LEEF**—UserEdited
- **Syslog**—UserEdited
- **Email**—UserEdited

User Status Changed | The status of an administrative user was changed.
- **CEF**—UserStatusChanged
- **LEEF**—UserStatusChanged
- **Syslog**—UserStatusChanged
- **Email**—UserStatusChanged
## Settings - Agent

The following table displays the agent settings logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent One Time Action Completed</td>
<td>An agent has finished running an action rule on an endpoint.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>OneTimeActionComplete</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>OneTimeActionComplete</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>OneTimeActionComplete</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>OneTimeActionComplete</em></td>
</tr>
<tr>
<td>Agent One Time Action Failed</td>
<td>An agent failed to run an action rule on an endpoint.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>OneTimeActionFailed</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>OneTimeActionFailed</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>OneTimeActionFailed</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>OneTimeActionFailed</em></td>
</tr>
<tr>
<td>File Restore Failed</td>
<td>An agent failed to restore a file to its original location on the endpoint or attached removable media.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>RestoreFailed</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>RestoreFailed</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>RestoreFailed</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>RestoreFailed</em></td>
</tr>
<tr>
<td>File Quarantine Failed</td>
<td>An agent failed to quarantine a file on the endpoint or its attached removable media.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>QuarantineFailed</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>QuarantineFailed</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>QuarantineFailed</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>QuarantineFailed</em></td>
</tr>
<tr>
<td>File Restore Succeeded</td>
<td>An agent successfully restored a file to its original location on the endpoint or attached removable media.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>RestoreSucceeded</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>RestoreSucceeded</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>RestoreSucceeded</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>RestoreSucceeded</em></td>
</tr>
<tr>
<td>File Quarantine Succeeded</td>
<td>An agent successfully quarantined a file on the endpoint or its attached removable media.</td>
</tr>
<tr>
<td></td>
<td>• CEF—<em>QuarantineSucceeded</em></td>
</tr>
<tr>
<td></td>
<td>• LEEF—<em>QuarantineSucceeded</em></td>
</tr>
<tr>
<td></td>
<td>• Syslog—<em>QuarantineSucceeded</em></td>
</tr>
<tr>
<td></td>
<td>• Email—<em>QuarantineSucceeded</em></td>
</tr>
</tbody>
</table>
**Settings - ESM**

The following table displays the ESM settings logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESM Items Deleted</td>
<td>A security event was removed from the ESM Console.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ArchivedPreventions</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ArchivedPreventions</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ArchivedPreventions</td>
</tr>
<tr>
<td></td>
<td>• Email—ArchivedPreventions</td>
</tr>
<tr>
<td>ESM Items Deleted Failed</td>
<td>The ESM Console failed to remove a security event.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ArchivedPreventionsFailure</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ArchivedPreventionsFailure</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ArchivedPreventionsFailure</td>
</tr>
<tr>
<td></td>
<td>• Email—ArchivedPreventionsFailure</td>
</tr>
<tr>
<td>Settings Changed</td>
<td>The ESM Console settings have changed.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ConfigurationChange</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ConfigurationChange</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ConfigurationChange</td>
</tr>
<tr>
<td></td>
<td>• Email—ConfigurationChange</td>
</tr>
</tbody>
</table>

**Settings - Conditions**

The following table displays the condition management logs you can forward to an external logging platform or email.

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Added/Edited</td>
<td>A condition was added or edited.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ConditionEdited</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ConditionEdited</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ConditionEdited</td>
</tr>
<tr>
<td></td>
<td>• Email—ConditionEdited</td>
</tr>
<tr>
<td>Condition Deleted</td>
<td>A condition was deleted.</td>
</tr>
<tr>
<td></td>
<td>• CEF—ConditionDeleted</td>
</tr>
<tr>
<td></td>
<td>• LEEF—ConditionDeleted</td>
</tr>
<tr>
<td></td>
<td>• Syslog—ConditionDeleted</td>
</tr>
<tr>
<td></td>
<td>• Email—ConditionDeleted</td>
</tr>
</tbody>
</table>

**Settings - Licenses**

The following table displays the license management logs you can forward to an external logging platform or email.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent License Validation Failed</td>
<td>The agent failed to validate the license.</td>
</tr>
<tr>
<td></td>
<td>- CEF—MachineLicenseValidationFailed</td>
</tr>
<tr>
<td></td>
<td>- LEEF—MachineLicenseValidationFailed</td>
</tr>
<tr>
<td></td>
<td>- Syslog—MachineLicenseValidationFailed</td>
</tr>
<tr>
<td></td>
<td>- Email—MachineLicenseValidationFailed</td>
</tr>
<tr>
<td>License Expiration</td>
<td>The license expired on the agent.</td>
</tr>
<tr>
<td></td>
<td>- CEF—LicenseExpiration</td>
</tr>
<tr>
<td></td>
<td>- LEEF—LicenseExpiration</td>
</tr>
<tr>
<td></td>
<td>- Syslog—LicenseExpiration</td>
</tr>
<tr>
<td></td>
<td>- Email—LicenseExpiration</td>
</tr>
<tr>
<td>License Quantity</td>
<td>The number of licenses has changed.</td>
</tr>
<tr>
<td></td>
<td>- CEF—LicenseQuantity</td>
</tr>
<tr>
<td></td>
<td>- LEEF—LicenseQuantity</td>
</tr>
<tr>
<td></td>
<td>- Syslog—LicenseQuantity</td>
</tr>
<tr>
<td></td>
<td>- Email—LicenseQuantity</td>
</tr>
<tr>
<td>Agent License Request</td>
<td>The agent requested a license.</td>
</tr>
<tr>
<td></td>
<td>- CEF—ClientLicenseRequest</td>
</tr>
<tr>
<td></td>
<td>- LEEF—ClientLicenseRequest</td>
</tr>
<tr>
<td></td>
<td>- Syslog—ClientLicenseRequest</td>
</tr>
<tr>
<td></td>
<td>- Email—ClientLicenseRequest</td>
</tr>
<tr>
<td>Agent License Invalid</td>
<td>The license on the agent was invalid.</td>
</tr>
<tr>
<td></td>
<td>- CEF—ClientLicenseInvalid</td>
</tr>
<tr>
<td></td>
<td>- LEEF—ClientLicenseInvalid</td>
</tr>
<tr>
<td></td>
<td>- Syslog—ClientLicenseInvalid</td>
</tr>
<tr>
<td></td>
<td>- Email—ClientLicenseInvalid</td>
</tr>
<tr>
<td>License Sent to Agent</td>
<td>The agent received a new license.</td>
</tr>
<tr>
<td></td>
<td>- CEF—SendingLicenseToClient</td>
</tr>
<tr>
<td></td>
<td>- LEEF—SendingLicenseToClient</td>
</tr>
<tr>
<td></td>
<td>- Syslog—SendingLicenseToClient</td>
</tr>
<tr>
<td></td>
<td>- Email—SendingLicenseToClient</td>
</tr>
<tr>
<td>License Pool Added</td>
<td>A new pool of licenses was added to the ESM Console.</td>
</tr>
<tr>
<td></td>
<td>- CEF—LicensePoolAdded</td>
</tr>
<tr>
<td></td>
<td>- LEEF—LicensePoolAdded</td>
</tr>
<tr>
<td></td>
<td>- Syslog—LicensePoolAdded</td>
</tr>
<tr>
<td></td>
<td>- Email—LicensePoolAdded</td>
</tr>
<tr>
<td>Agent License Revoked</td>
<td>The license for an agent was revoked.</td>
</tr>
<tr>
<td></td>
<td>- CEF—LicenseRevoked</td>
</tr>
<tr>
<td></td>
<td>- LEEF—LicenseRevoked</td>
</tr>
<tr>
<td>Event Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>• Syslog—LicenseRevoked</td>
<td></td>
</tr>
<tr>
<td>• Email—LicenseRevoked</td>
<td></td>
</tr>
</tbody>
</table>
Common Variables Used in Events

From the ESM Console, you can configure log forwarding for the events that matter to you most. The ESM translates event information into the format of your choice and sends it to the external logging platform and optionally to an email address. Included in each event are variables which the ESM replaces with values to make each event meaningful. Many variables are shared across similar types of events. The following topics describe some of the most common variables by the type of event:

- Agent Change Event Variables
- ESM Configuration Change Event Variables
- Policy Change Event Variables
- ESM Server Event Variables
- Security Event Monitoring Variables

Agent Change Event Variables

Agent change events occur on the endpoint and include changes to content updates, licenses, software, connection status, one-time action rules, processes and services, and quarantined files. The ESM Console lists these events under the **Monitor - Agent** Logging Events category. The following table displays the most commonly specified variables in agent-related events.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhost</td>
<td>Machine name of the endpoint</td>
</tr>
<tr>
<td>duser</td>
<td>User who is logged in to the endpoint</td>
</tr>
<tr>
<td>msg</td>
<td>Description of the nature of the event</td>
</tr>
<tr>
<td>Module</td>
<td>Name of the exploit protection module (EPM)</td>
</tr>
<tr>
<td>ContentVersion</td>
<td>Content update version</td>
</tr>
<tr>
<td>ModuleVersion</td>
<td>Local analysis module version</td>
</tr>
</tbody>
</table>

For example, consider the output for an **Agent Service Start** event in CEF format:

```
```

Notice that this event uses several common variables, namely: **dhost**, **duser**, and **msg**.

ESM Configuration Change Event Variables

ESM configuration change events include system-wide changes to licensing, administrative users and roles, processes, restriction settings, and conditions. The ESM Console lists these events under the following Logging Events categories:
• Policies - Process Management
• Policies - Restriction Settings
• Settings - Administration
• Settings Conditions

The following table displays the most commonly specified variables in ESM configuration-related events.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>shost</td>
<td>Machine name of the ESM Console server</td>
</tr>
<tr>
<td>suser</td>
<td>User who is logged in to the ESM Console</td>
</tr>
<tr>
<td>msg</td>
<td>Free text description</td>
</tr>
<tr>
<td>dhost</td>
<td>Machine name of the endpoint</td>
</tr>
<tr>
<td>deviceProcessName</td>
<td>Process name</td>
</tr>
</tbody>
</table>

For example, consider the output for a Role Added/Edited event in CEF format:

```
Sep 28 2016 17:42:04 ESM CEF:0|Palo Alto Networks|Traps ESM|3.4.1.16709|Role Edited|Config|3|rt=Sep 28 2016 17:42:04 shost=ESM suser=administrator
msg=Role TechWriter was added\changed
```

Notice that this event uses several common variables, namely: shost, suser, and msg.

Policy Change Event Variables

Policy change events include changes to rules, protection levels, content updates, and verdicts. The ESM Console lists these events under the following Logging Events categories:

• Policies - General
• Policies - Rules
• Policies - Hash Control

The following table displays the most commonly specified variables in policy change events.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>shost</td>
<td>Machine name of the ESM Console server</td>
</tr>
<tr>
<td>suser</td>
<td>User who is logged in to the ESM Console</td>
</tr>
<tr>
<td>fileHash</td>
<td>Hash value of an executable file</td>
</tr>
<tr>
<td>msg</td>
<td>Free text description</td>
</tr>
</tbody>
</table>

For example, consider the output of a Hash Added event in CEF format:

```
Sep 28 2016 17:34:56 172.16.183.173 CEF:0|Palo
ESM Server Event Variables

ESM Server events include changes related to preventions, configuration changes, ESM status, licenses, ESM Tech Support files, communication with WildFire. The ESM Console lists these events under the following logging categories:

- Settings - ESM
- Settings - Licenses
- Monitor - ESM

The following table displays the most commonly specified variables in ESM Server-related events.

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>shost</td>
<td>Machine name of the ESM Console server</td>
</tr>
<tr>
<td>suser</td>
<td>User who is logged in to the ESM Console</td>
</tr>
<tr>
<td>dhost</td>
<td>Machine name of the endpoint</td>
</tr>
<tr>
<td>msg</td>
<td>Free text description message</td>
</tr>
<tr>
<td>duser</td>
<td>User who is logged in to the endpoint</td>
</tr>
<tr>
<td>FileName</td>
<td>Executable filename</td>
</tr>
</tbody>
</table>

For example, consider the following output for a Communication Check With Proxy event in CEF format:

```
Sep 28 2016 17:34:50 172.16.183.173 CEF:0|Palo Alto Networks|Traps ESM|3.4.1.16709|Communications Check With Proxy|System|9|rt=Sep
28 2016 17:34:50 shost=ESM suser= dhost=ESM msg=Communications check with Proxy on host 'ESM'. Status: 'WildFire communication succeeded, proxy is disabled.'
```

Notice that this event uses several common variables, namely: shost, dhost, and msg.

Security Event Monitoring Variables

Security events include all prevention, notification, and provisional events that are reported by the Traps agents. The ESM Console lists these events under the Security Events Logging Events category. The following table displays the most commonly specified variables used for monitoring security events.

Notice that this event uses several common variables, namely: shost, suser, fileHash, and msg.
### Name | Meaning
---|---
dhost | Machine name of the endpoint
duser | User that was logged onto the endpoint.
Model | Name of the exploit protection module (EPM)
deviceProcessName | Process name
File Hash | Hash value of an executable file
dvc/dst | IP address of the endpoint
msg | Free text description
Content Version | Content version

For example, consider the output of a **Prevention Event** in CEF format:


Notice that this event uses several common variables, namely: dhost, duser, deviceProcessName, fileHash, dvc, and msg.
Forward Logs to an External Logging Platform

Syslog is a standard log transport mechanism that enables the aggregation of log data from different network devices and vendors into a central repository for archive, analysis, and reporting. Depending on the type and severity of the data in the log files, you may want to receive alerts for critical events that require your attention, or you may have policies that require you to archive the data for longer than it can be stored on the ESM Console. In these cases, you can configure the ESM to forward your log data to an external service for archive, notification, analysis, or any combination of the three.

- Enable Log Forwarding to an External Logging Platform
- Enable Log Forwarding to an External Logging Platform Using the DB Configuration Tool
- CEF Format
- LEEF Format
- Syslog (RFC5424) Format

Enable Log Forwarding to an External Logging Platform

The ESM Console and ESM Servers collectively generate logs for over 60 types of events—including security events, policy configuration changes, and monitoring events (agent and server)—that can be forwarded to an external logging platform. By enabling log forwarding the ESM can forward all or some of these logs to an external service for long-term storage and analysis.

The ESM component which forwards the logs varies depending on the type of event. For example, if you monitor verdict changes, the ESM Console sends logs when you override the verdict for a hash. If WildFire changes the verdict, the ESM Server sends the logs.

To send logs, use TCP or SSL for reliable and secure transport of logs, or UDP for non-secure transport. You can also customize the information format (CEF, LEEF, or Syslog) that the ESM uses to send the logs.

*The date/time of the each logged event is in UTC.*

**STEP 1** | Enable log forwarding.

From the ESM Console, select **Settings > ESM > Syslog**, and then **Enable Syslog**.

**STEP 2** | Configure the settings to send logs from ESM components to an external logging platform. To send logs to an email, see **Forward Logs to Email**.

Configure the following settings:

- **Syslog Server**—Hostname or IP address of the external logging platform.
- **Syslog Port**—Communication port of the external logging platform, such as 514.
- **Syslog Protocol**—The format the ESM uses to send reports: **CEF**, **LEEF**, or **Syslog**.
- **Keep-alive Timeout**—Period (in minutes) in which Traps sends a keep-alive message to the external logging platform (default is 0; range is 0 to 2,147,483,647). A value of 0 specifies that you do not want to send a keep-alive message to the external logging platform.
- **Communication Protocol**—Transport layer protocol that the ESM uses to send syslog reports: **TCP**, **TCP with SSL**, or **UDP**.

**STEP 3** | Select the events that you want to send to the external logging platform.

In the Logging Events area, select one or more of the events. Scroll through the list to see additional types of events you can send.
Enable Log Forwarding to an External Logging Platform Using the DB Configuration Tool

The Endpoint Security Manager can write logs to an external logging platform, such as security information and event management (SIEM), Service Organization Controls (SOCs), or syslog, in addition to storing its logs internally. Specifying an external logging platform allows you to view aggregated logs from all ESM Servers. You can enable external reporting using the Endpoint Security Manager (see Forward Logs to an External Logging Platform) or using the Database (DB) Configuration Tool.

The DB Configuration Tool is a command-line interface that provides an alternative to managing basic server settings using the ESM Console. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt run as an administrator. The DB Configuration Tool is located in the Server folder on the ESM Server.

All commands run using the DB Configuration Tool are case sensitive.

By default, log forwarding is disabled.

STEP 1 | Open a command prompt as an administrator:

- Select Start > All Programs > Accessories. Right-click Command prompt, and then select Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

STEP 2 | Navigate to the folder that contains the DB Configuration Tool:

C:\Users\Administrator> cd
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server

STEP 3 | (Optional) View the existing reporting settings:

C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting show
EnableSyslog = False
SyslogServer =
SyslogPort = 0
SyslogProtocol = Cef
KeepAliveTimeout = 0
MaximumReportsCount = 500000
MinReportsCount = 450000
SyslogCommunicationType = Udp
STEP 4 | Enable log forwarding to an external logging platform such as a syslog server:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting EnableSyslog true
```

STEP 5 | Specify the IP address (or hostname) of the external logging platform:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting SyslogServer <ipaddress>
```

STEP 6 | Specify the communication port for the external logging platform, a value between 1 and 65535 (default is 514):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting SyslogPort <portnumber>
```

STEP 7 | Specify the protocol that the ESM Console will use to send reports, either Cef, Leef, or Rfc5424 (syslog).

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting SyslogProtocol [Cef | Leef | Rfc5424]
```

STEP 8 | (Optional) Specify a timespan (in minutes) where the endpoint sends a keep alive message to the log or report, a value of 0 or greater (default is 0):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting KeepAliveTimeout <value>
```

STEP 9 | (Optional) Specify the maximum number of report notifications to store in the database, a value of 0 or greater (default is 4000):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting MaximumReportsCount <value>
```

For example, specifying a maximum report count of 5000 notifications means the Endpoint Security Manager will discard older notifications higher than 5000.

STEP 10 | (Optional) Specify the minimum number of report notifications to store in the database, a value of 0 or greater (default is 5000):

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig reporting MinReportsCount <value>
```

**CEF Format**

The following table lists the events in CEF format.
<table>
<thead>
<tr>
<th>Event</th>
<th>CEF Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessViolation</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>AgentContentUpdate</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>AgentPolicyChange</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ArchivedPreventions</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ArchivedPreventionsFailure</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ClientInstall</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ClientLicenseInvalid</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ClientLicenseRequest</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ClientUninstall</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ClientUpgrade</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>CommunicationsCheckWithProxy</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ConditionDeleted</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ConditionEdited</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ConfigurationChange</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>DisabledProtection</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Protection Disabled</strong></td>
<td>Protection Disabled</td>
</tr>
<tr>
<td><strong>EnabledProtection</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td><strong>EndpointDisconnected</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td><strong>EsmConfigurationChange</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td><strong>EsmStatusChange</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td><strong>FileUploadFailure</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td><strong>HashesImport</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td><strong>Heartbeat</strong></td>
<td>@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>LicenseExpiration</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>LicensePoolAdded</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>LicenseQuantity</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>LicenseRevoked</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>LocalAnalysisFeatureExtractionFailed</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>LocalAnalysisModelUnavailable</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>LocalAnalysisModuleFailed</td>
<td>`@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>@Model.ExternalSeverity</td>
</tr>
<tr>
<td>LocalAnalysisModuleSucceeded</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>MachineLicenseValidationFailed</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>NewHash</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>NotificationEvent</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>OneTimeActionComplete</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>OneTimeActionFailed</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>PostDetectionEvent</td>
<td><code>duser=@Model[&quot;user&quot;] msg=One Time Action failed to run. Action Type: @Model[&quot;ActionType&quot;]</code></td>
</tr>
<tr>
<td>PreventionEvent</td>
<td><code>dhost=@Model[&quot;host&quot;] duser=@Model[&quot;user&quot;] cs2Label=Module cs2=@Model[&quot;EPM&quot;] deviceProcessName=@Model[&quot;ProcessName&quot;] fileHash=@Model[&quot;Hash&quot;] cs3Label=ContentVersion cs3=@Model[&quot;ContentVersion&quot;] dvc=@Model[&quot;AgentIp&quot;] msg=New post detection event. Prevention Key: @Model[&quot;preventionKey&quot;]</code></td>
</tr>
<tr>
<td>ProcessCrashed</td>
<td><code>dhost=@Model[&quot;host&quot;] duser=@Model[&quot;user&quot;] msg=Process @Model[&quot;ProcessName&quot;] had crashed</code></td>
</tr>
<tr>
<td>ProcessDeleted</td>
<td><code>shost=@Model[&quot;esmHost&quot;] suser=@Model[&quot;user&quot;] deviceProcessName=@Model[&quot;Name&quot;] msg=Process was deleted</code></td>
</tr>
<tr>
<td>ProcessEdited</td>
<td><code>deviceProcessName=@Model.Data.ProcessFilename msg=Process was added/edited</code></td>
</tr>
<tr>
<td>ProcessInjectionTimedOut</td>
<td><code>dhost=@Model[&quot;host&quot;] duser=@Model[&quot;user&quot;] cs2Label=Module cs2=@Model[&quot;EPM&quot;] deviceProcessName=@Model[&quot;ProcessName&quot;] fileHash=@Model[&quot;Hash&quot;] cs3Label=ContentVersion cs3=@Model[&quot;ContentVersion&quot;] dvc=@Model[&quot;AgentIp&quot;] msg=New prevention event. Prevention Key: @Model[&quot;preventionKey&quot;]</code></td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ProvisionalEvent              | @Model["Time"] @Model["EsmIp"] CEF:0 | Palo Alto Networks|Traps Agent|@Model["ProductVersion"]|Provisional Event|Threat|@Model.ExternalSeverity|rt=@Model["Time"]
dhost=@Model["host"] duser=@Model["user"]
msg=New provisional event. Prevention Key: @Model["preventionKey"] |
| PublisherChanged              | @Model["Time"] @Model["EsmIp"] CEF:0 | Palo Alto Networks|Traps ESM|@Model["ProductVersion"]|Trusted Signer Changed|Policy|@Model.ExternalSeverity|rt=@Model["Time"]
shost=@Model["esmHost"]
suser=@Model["user"]
fileHash=@Model["Hash"]
msg=Hash @Model["Hash"] trusted signer changed automatically from @Model["OldPublisher"] to @Model["NewPublisher"] |
| QuarantineFailed              | @Model["Time"] @Model["EsmIp"] CEF:0 | Palo Alto Networks|Traps Agent|@Model["ProductVersion"]|Quarantine Failed|Agent|@Model.ExternalSeverity|rt=@Model["Time"]
dhost=@Model["host"]
duser=@Model["user"]
msg=File @Model["fileName"] could not be quarantined, reason: @Model["FailureReason"] |
| QuarantineQuotaExceeded       | @Model["Time"] @Model["EsmIp"] CEF:0 | Palo Alto Networks|Traps Agent|@Model["ProductVersion"]|Quarantine Quota Exceeded |Agent|@Model.ExternalSeverity|rt=@Model["Time"]
dhost=@Model["host"]
duser=@Model["user"]
msg=File @Model["fileName"] was permanently removed from the quarantine folder because quota was exceeded |
| QuarantineSucceeded           | @Model["Time"] @Model["EsmIp"] CEF:0 | Palo Alto Networks|Traps Agent|@Model["ProductVersion"]|Quarantine Succeeded |Agent|@Model.ExternalSeverity|rt=@Model["Time"]
dhost=@Model["host"]
duser=@Model["user"]
msg=File @Model["fileName"] was quarantined successfully |
<p>| ReportingServiceStartFailed   | @Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0 | Palo Alto Networks|Traps Agent|@Model[&quot;ProductVersion&quot;]|Reporting Service Start Failed|Agent|@Model.ExternalSeverity|rt=@Model[&quot;Time&quot;] |</p>
<table>
<thead>
<tr>
<th>Event</th>
<th>CEF Format</th>
</tr>
</thead>
</table>
| RestoreFailed            | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps Agent | @Model["ProductVersion"]| Restore Failed| Agent | @Model.ExternalSeverity| rt=@Model["Time"]
|                          | dhost=@Model["host"] duser=@Model["user"] msg=File @Model["fileName"] could not be restored, reason: @Model["FailureReason"]                                                                                           |
| RestoreSucceeded         | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps Agent | @Model["ProductVersion"]| Restore Succeeded| Agent | @Model.ExternalSeverity| rt=@Model["Time"]
|                          | dhost=@Model["host"] duser=@Model["user"] msg=File @Model["fileName"] restored successfully                                                                                                           |
| RestrictionSettingsEdited | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps ESM | @Model["ProductVersion"]| Restriction Settings Edited| Config | @Model.ExternalSeverity| rt=@Model["Time"]
|                          | shost=@Model["esmHost"] suser=@Model["user"] msg=Restriction Settings were added/changed                                                                                                                      |
| RoleDeleted              | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps ESM | @Model["ProductVersion"]| Role Deleted | Config | @Model.ExternalSeverity| rt=@Model["Time"]
|                          | shost=@Model["esmHost"] suser=@Model["user"] msg=Role @Model["Name"] was deleted                                                                                                                      |
| RoleEdited               | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps ESM | @Model["ProductVersion"]| Role Edited | Config | @Model.ExternalSeverity| rt=@Model["Time"]
|                          | shost=@Model["esmHost"] suser=@Model["user"] msg=Role @Model.Data.Name was added/changed                                                                                                                  |
| RoleStatusChanged        | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps ESM | @Model["ProductVersion"]| Role Status Changed | Config | @Model.ExternalSeverity| rt=@Model["Time"]
|                          | shost=@Model["esmHost"] suser=@Model["user"] msg=Role @Model["Name"] status was changed to @Model["Status"]                                                                                     |
| RuleDeleted              | @Model["Time"] @Model["EsmIp"] CEF:0| Palo Alto Networks| Traps ESM | @Model["ProductVersion"]| Rule Deleted | Policy | @Model.ExternalSeverity| rt=@Model["Time"]
<p>|                          | suser=@Model[&quot;user&quot;] cs1Label=Rule cs1=@Model[&quot;id&quot;] msg=Rule @Model[&quot;id&quot;]: Deleted                                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Event</th>
<th>CEF Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>RuleEdited</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>SendingLicenseToClient</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServerContentRevertFailure</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServerContentRevertSuccess</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServerContentUpdateFailure</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServerContentUpdateSuccess</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServerHeartbeat</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServiceAlive</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServiceStartFailed</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServiceStopped</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>ServiceWarning</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>SystemShutdown</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>TechSupportFileStatus</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>TrapsServiceStatusChange</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>UserDeleted</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UserEdited</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>UserLogin</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>UserStatusChanged</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>VerdictChange</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>VerdictChangeAnyToMalware</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>VerdictChangeMalwareToAny</td>
<td>@Model[&quot;Time&quot;] @Model[&quot;EsmIp&quot;] CEF:0</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
<tr>
<td>Event</td>
<td>CEF Format</td>
</tr>
</tbody>
</table>
## LEEF Format

The following table lists the events in LEEF format.

<table>
<thead>
<tr>
<th>Event</th>
<th>LEEF Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessViolation</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>AgentContentUpdate</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>AgentPolicyChange</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ArchivedPreventions</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ArchivedPreventionsFailure</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ClientInstall</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>duser=Model[&quot;user&quot;] msg=Agent installed sev=Model.ExternalSeverity</td>
</tr>
<tr>
<td>ClientLicenseInvalid</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ClientLicenseRequest</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ClientUninstall</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ClientUpgrade</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>CommunicationsCheckWithProxy</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ConditionDeleted</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ConditionEdited</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConfigurationChange</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>
|   | @Model["ProductVersion"]|Settings Change|cat=Config subtype=Settings Change devTime=@Model["Time"]  
|   | src=@Model["EsmIp"]|shost=@Model["esmHost"]|suser=@Model["user"]|dhost=@Model["host"]|msg=@Model["Property"] has changed from @Model["OldValue"] to @Model["NewValue"]. |
| DisabledProtection    | LEEF:1.0|Palo Alto Networks|Traps ESM|  
|   | @Model["ProductVersion"]|Protection Disabled|cat=Policy subtype=Protection Disabled devTime=@Model["Time"]  
|   | src=@Model["EsmIp"]|shost=@Model["esmHost"]|suser=@Model["user"]|msg=Protection disabled on all agents |
| EnabledProtection     | LEEF:1.0|Palo Alto Networks|Traps Agent|  
|   | @Model["ProductVersion"]|Endpoint Disconnected|cat=Agent subtype=Endpoint Disconnected devTime=@Model["Time"]  
|   | src=@Model["EsmIp"]|dhost=@Model["host"]|duser=@Model["user"]|msg=Agent disconnected. last HB @Model["lastHBTime"] |
| EsmConfigurationChange| LEEF:1.0|Palo Alto Networks|Traps ESM|  
|   | @Model["ProductVersion"]|ESM Configuration Change|cat=System subtype=ESM Configuration Change devTime=@Model["Time"]  
|   | src=@Model["EsmIp"]|shost=@Model["esmHost"]|suser=@Model["user"]|dhost=@Model["host"]|msg=Multi ESM configurations has changed sev=@Model.ExternalSeverity |
| EsmStatusChange       | LEEF:1.0|Palo Alto Networks|Traps ESM|  
|   | @Model["ProductVersion"]|ESM Status Change|cat=System subtype=ESM Status Change devTime=@Model["Time"]  
|   | src=@Model["EsmIp"]|shost=@Model["esmHost"]|suser=@Model["user"]|dhost=@Model["host"]|msg=ESM status changed sev=@Model.ExternalSeverity |
| FileUploadFailure     | LEEF:1.0|Palo Alto Networks|Traps ESM|  
|   | @Model["ProductVersion"]|File Upload Failure|cat=System subtype=File Upload Failure devTime=@Model["Time"]  
<p>|   | src=@Model[&quot;EsmIp&quot;]|shost=@Model[&quot;esmHost&quot;]|suser=@Model[&quot;user&quot;]|dhost=@Model[&quot;host&quot;]|duser=@Model[&quot;user&quot;]|fname=@Model[&quot;fileName&quot;]|msg=File failed to upload sev=@Model.ExternalSeverity |</p>
<table>
<thead>
<tr>
<th>Event</th>
<th>LEEF Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>HashesImport</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>LicenseExpiration</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>LicensePoolAdded</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>LicenseQuantity</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>LicenseRevoked</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>LocalAnalysisFeatureExtractionFailed</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Failed</td>
<td><code>Failed devTime=@Model[&quot;Time&quot;] src=@Model[&quot;EsmIp&quot;] dhost=@Model[&quot;host&quot;] duser=@Model[&quot;user&quot;] ContentVersion=@Model[&quot;ContentVersion&quot;] msg=Local Analysis Feature Extraction Failed sev=@Model.ExternalSeverity</code></td>
</tr>
<tr>
<td>LocalAnalysisModelUnavailable</td>
<td>`LEEF:1.0</td>
</tr>
<tr>
<td>LocalAnalysisModuleFailed</td>
<td>`LEEF:1.0</td>
</tr>
<tr>
<td>LocalAnalysisModuleSucceeded</td>
<td>`LEEF:1.0</td>
</tr>
<tr>
<td>MachineLicenseValidationFailed</td>
<td>`LEEF:1.0</td>
</tr>
<tr>
<td>NewHash</td>
<td>`LEEF:1.0</td>
</tr>
<tr>
<td>NotificationEvent</td>
<td>`LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>Event <code>devTime=@Model[&quot;Time&quot;]</code> <code>src=@Model[&quot;EsmIp&quot;]</code> <code>dhost=@Model[&quot;host&quot;]</code> <code>duser=@Model[&quot;user&quot;]</code> <code>Module=@Model[&quot;EPM&quot;]</code> <code>deviceProcessName=@Model[&quot;ProcessName&quot;]</code> <code>fileHash=@Model[&quot;Hash&quot;]</code> <code>ContentVersion=@Model[&quot;ContentVersion&quot;]</code> <code>dst=@Model[&quot;AgentIp&quot;]</code> <code>msg=New notification event. Prevention Key: @Model[&quot;preventionKey&quot;]</code> <code>sev=@Model.ExternalSeverity</code></td>
</tr>
<tr>
<td>OneTimeActionComplete</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>OneTimeActionFailed</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>PostDetectionEvent</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>PreventionEvent</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>ProcessCrashed</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td>cat=Agent</td>
</tr>
<tr>
<td></td>
<td>devTime=@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td></td>
<td>dhost=@Model[&quot;host&quot;]</td>
</tr>
<tr>
<td></td>
<td>msg=Process @Model[&quot;ProcessName&quot;] had crashed</td>
</tr>
<tr>
<td></td>
<td>sev=@Model.ExternalSeverity</td>
</tr>
<tr>
<td>ProcessDeleted</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td>cat=Config</td>
</tr>
<tr>
<td></td>
<td>devTime=@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td></td>
<td>shost=@Model[&quot;esmHost&quot;]</td>
</tr>
<tr>
<td></td>
<td>deviceProcessName=@Model[&quot;Name&quot;]</td>
</tr>
<tr>
<td></td>
<td>sev=@Model.ExternalSeverity</td>
</tr>
<tr>
<td>ProcessEdited</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td>cat=Config</td>
</tr>
<tr>
<td></td>
<td>devTime=@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td></td>
<td>shost=@Model[&quot;esmHost&quot;]</td>
</tr>
<tr>
<td></td>
<td>deviceProcessName=@Model.Data.ProcessFilename</td>
</tr>
<tr>
<td></td>
<td>sev=@Model.ExternalSeverity</td>
</tr>
<tr>
<td>ProcessInjectionTimedOut</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td>cat=Agent</td>
</tr>
<tr>
<td></td>
<td>devTime=@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td></td>
<td>dhost=@Model[&quot;host&quot;]</td>
</tr>
<tr>
<td></td>
<td>msg=Injection Timeout</td>
</tr>
<tr>
<td>ProvisionalEvent</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td>cat=Threat</td>
</tr>
<tr>
<td></td>
<td>devTime=@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td></td>
<td>dhost=@Model[&quot;host&quot;]</td>
</tr>
<tr>
<td></td>
<td>Module=@Model[&quot;EPM&quot;]</td>
</tr>
<tr>
<td></td>
<td>fileHash=@Model[&quot;Hash&quot;]</td>
</tr>
<tr>
<td></td>
<td>dst=@Model[&quot;AgentIp&quot;]</td>
</tr>
<tr>
<td></td>
<td>sev=@Model.ExternalSeverity</td>
</tr>
<tr>
<td>PublisherChanged</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td></td>
<td>cat=Policy</td>
</tr>
<tr>
<td></td>
<td>devTime=@Model[&quot;Time&quot;]</td>
</tr>
<tr>
<td></td>
<td>shost=@Model[&quot;esmHost&quot;]</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>QuarantineFailed</td>
<td>fileHash=@Model[&quot;Hash&quot;] msg=Hash @Model[&quot;Hash&quot;] trusted signer changed automatically from @Model[&quot;OldPublisher&quot;] to @Model[&quot;NewPublisher&quot;] sev=@Model.ExternalSeverity</td>
</tr>
<tr>
<td>QuarantineQuotaExceeded</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>QuarantineSucceeded</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ReportingServiceStartFailed</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RestoreFailed</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RestoreSucceeded</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>msg=File @Model[&quot;fileName&quot;] restored successfully  sev=@Model.ExternalSeverity</td>
</tr>
<tr>
<td>RestrictionSettingsEdited</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RoleDeleted</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RoleEdited</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RoleStatusChanged</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RuleDeleted</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>RuleEdited</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>SendingLicenseToClient</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><code>dhost=@Model[&quot;host&quot;] msg=New license sent sev=@Model.ExternalSeverity</code></td>
</tr>
<tr>
<td>ServerContentRevertFailure</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServerContentRevertSuccess</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServerContentUpdateFailure</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServerContentUpdateSuccess</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServerHeartbeat</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServiceAlive</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServiceStartFailed</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServiceStopped</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>ServiceWarning</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>SystemShutdown</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>TechSupportFileStatus</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>TrapsServiceStatusChange</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>UserDeleted</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UserEdited</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>UserLogin</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>UserStatusChanged</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>VerdictChange</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>VerdictChangeAnyToMalware</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>VerdictChangeMalwareToAny</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>Event</td>
<td>LEEF Format</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>VerdictChangeNoConnectionToAny</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>VerdictChangeUnknownToAny</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>VerdictManualOverride</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>VerdictRevertedToWildfire</td>
<td>LEEF:1.0</td>
</tr>
<tr>
<td>WfCommunicationsStatusChanged</td>
<td>LEEF:1.0</td>
</tr>
</tbody>
</table>
### Syslog (RFC5424) Format

The following table lists the events in syslog (RFC5424) format.

<table>
<thead>
<tr>
<th>Event</th>
<th>Syslog Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessViolation</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Threat, Access Violation, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Access Violation- @Model[&quot;TargetName&quot;]: @Model[&quot;TargetValue&quot;], @Model.ExternalSeverity, @Model[&quot;EPM&quot;],,,</td>
</tr>
<tr>
<td>AgentContentUpdate</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Agent Content Update, @Model[&quot;host&quot;], @Model[&quot;user&quot;], @Model[&quot;host&quot;] received new content- version @Model[&quot;ContentVersion&quot;], @Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>AgentPolicyChange</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Agent Policy Changed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Policy changed, @Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>ArchivedPreventions</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, Preventions Archived, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], @Model[&quot;host&quot;], ,@Model[&quot;totalPreventions&quot;] prevented been archived, @Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>ArchivedPreventionsFailure</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, Preventions Archived Failed, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], ,, Archived preventions failed, @Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>ClientInstall</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Agent Install, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Agent installed, @Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>ClientLicenseInvalid</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Client License Invalid, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Invalid license , @Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>ClientLicenseRequest</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| ClientUninstall             | `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps Agent, @Model["ProductVersion"], Agent, Agent Uninstall, @Model["host"], @Model["user"], Agent uninstalled, @Model.ExternalSeverity, , , , , ,        |
| ClientUpgrade               | `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps Agent, @Model["ProductVersion"], Agent, Agent Upgrade, @Model["host"], @Model["user"], Agent upgraded, @Model.ExternalSeverity, , , , , , |
| CommunicationsCheckWithProxy| `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps ESM, @Model["ProductVersion"], System, Communications Check With Proxy, @Model["esmHost"], @Model["user"], , , , Communications check with Proxy on host ' @Model["host"]'. Status: '@Model["message"]', @Model.ExternalSeverity, , , , , , |
| ConditionDeleted            | `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps ESM, @Model["ProductVersion"], Config, Condition Deleted, @Model["esmHost"], @Model["user"], , , , Condition ID: @Model["id"] was deleted, @Model.ExternalSeverity, , , , , , |
| ConditionEdited             | `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps ESM, @Model["ProductVersion"], Config, Condition Edited, @Model["esmHost"], @Model["user"], , , , Condition ID: @Model["id"] was added/changed., @Model.ExternalSeverity, , , , , , |
| ConfigurationChange         | `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps ESM, @Model["ProductVersion"], Config, Settings Change, @Model["esmHost"], @Model["user"], , , , @Model["Property"] has changed from @Model["OldValue"] to @Model["NewValue"], @Model.ExternalSeverity, , , , , , |
| DisabledProtection          | `<134>1 @Model["Rfc5424Time"]
@Model["EsmIp"] -- - @Model["Time"], Traps ESM, @Model["ProductVersion"], Policy, Protection Disabled, @Model["esmHost"], @Model["user"], Protection disabled on all agents, @Model.ExternalSeverity, , , , , , |
<table>
<thead>
<tr>
<th>Event</th>
<th>Syslog Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnabledProtection</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;],Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Endpoint disconnected, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Agent disconnected. last HB @Model[&quot;lastHBTime&quot;], @Model.ExternalSeverity, , , , , ,</td>
</tr>
<tr>
<td>EsmConfigurationChange</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, EPM Init Failed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], EPM @Model[&quot;EPM&quot;] failed to initialize, @Model.ExternalSeverity, , , , , ,</td>
</tr>
<tr>
<td>EsmStatusChange</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, ESM Configuration Change, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], , , , , , Multi ESM configurations has changed, @Model.ExternalSeverity, , , , , ,</td>
</tr>
<tr>
<td>FileUploadFailure</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Report to Windows Event Viewer, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Report to Windows Event Viewer, @Model.ExternalSeverity, , , , , ,</td>
</tr>
<tr>
<td>HashesImport</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, File Upload Failure, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], @Model[&quot;host&quot;], @Model[&quot;user&quot;], File failed to upload, @Model.ExternalSeverity, @Model[&quot;fileName&quot;], , , , , ,</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], Policy, Hashes Upload, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], @Model[&quot;Amount&quot;], hashes were uploaded, @Model.ExternalSeverity, @Model[&quot;Hash&quot;], , , , , ,</td>
</tr>
<tr>
<td>LicenseExpiration</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Heartbeat, @Model[&quot;host&quot;], Service is alive, @Model.ExternalSeverity, , , , , ,</td>
</tr>
<tr>
<td>LicensePoolAdded</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;Esmp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, License Expiration, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], , , @Model[&quot;user&quot;], @Model.ExternalSeverity, , , , , ,</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LicenseQuantity</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM, @Model[&quot;ProductVersion&quot;], System, License Pool Added, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], , , A pool of @Model[&quot;licenseCount&quot;] licenses of type @Model[&quot;licenseType&quot;] have been added, @Model.ExternalSeverity, , , ,</td>
</tr>
<tr>
<td>LicenseRevoked</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, License Quantity, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], , , , Agent Licenses are running low, @Model.ExternalSeverity, , , ,</td>
</tr>
<tr>
<td>LocalAnalysisFeatureExtractionFailed</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], Config, License Revoked, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], , @Model[&quot;host&quot;], Licenses revoked, @Model.ExternalSeverity, , , ,</td>
</tr>
<tr>
<td>LocalAnalysisModelUnavailable</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Local Analysis Extraction Failed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Local Analysis Feature Extraction Failed, @Model.ExternalSeverity, , , @Model[&quot;ContentVersion&quot;], , , ,</td>
</tr>
<tr>
<td>LocalAnalysisModuleFailed</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, Local Analysis Model Unavailable, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], @Model[&quot;host&quot;], , Local Analysis Model Unavailable, @Model.ExternalSeverity, , , ,</td>
</tr>
<tr>
<td>LocalAnalysisModuleSucceeded</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Local Analysis Module Failed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Add new module into Local Analysis- Failed, @Model.ExternalSeverity, , , ,</td>
</tr>
<tr>
<td>MachineLicenseValidationFailed</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Local Analysis Module Succeeded, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Add new module into Local Analysis- Failed, @Model.ExternalSeverity, , , ,</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>new module into Local Analysis- Succeeded, @Model.ExternalSeverity, [, @Model[&quot;ModuleVersion&quot;],</td>
<td></td>
</tr>
<tr>
<td>NewHash</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], System, Machine License Validation Failed, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], @Model[&quot;host&quot;], License Validation Failed, @Model.ExternalSeverity, [</td>
</tr>
<tr>
<td>NotificationEvent</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], Policy, New Hash Added, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], New hash added, @Model.ExternalSeverity, @Model[&quot;Hash&quot;], [, @Model[&quot;NewVerdict&quot;],</td>
</tr>
<tr>
<td>OneTimeActionComplete</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Threat, Notification Event, @Model[&quot;host&quot;], @Model[&quot;user&quot;], New notification event. Prevention Key: @Model[&quot;preventionKey&quot;], @Model.ExternalSeverity, @Model[&quot;EPM&quot;],</td>
</tr>
<tr>
<td>OneTimeActionFailed</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, One Time Action Complete, @Model[&quot;host&quot;], @Model[&quot;user&quot;], One Time Action completed. Action Type= @Model[&quot;ActionType&quot;]. Action ID= @Model[&quot;ActionID&quot;], @Model.ExternalSeverity, [</td>
</tr>
<tr>
<td>PostDetectionEvent</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, One Time Action Failed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], One Time Action failed to run. Action Type= @Model[&quot;ActionType&quot;], @Model.ExternalSeverity, [</td>
</tr>
<tr>
<td>PreventionEvent</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Threat, Post Detection Event, @Model[&quot;host&quot;], @Model[&quot;user&quot;], New post detection event. Prevention Key: @Model[&quot;preventionKey&quot;], @Model.ExternalSeverity, @Model[&quot;EPM&quot;],</td>
</tr>
<tr>
<td>ProcessCrashed</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmpIp&quot;] -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Threat, Prevention Event, @Model[&quot;host&quot;], @Model[&quot;user&quot;], New prevention event. Prevention Key: @Model[&quot;preventionKey&quot;], @Model.ExternalSeverity, @Model[&quot;EPM&quot;],</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ProcessDeleted</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Process Crashed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Process @Model[&quot;ProcessName&quot;] had crashed, @Model.ExternalSeverity, , , , ,</td>
</tr>
<tr>
<td>ProcessEdited</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], Config, Process Deleted, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], Process was deleted, @Model.ExternalSeverity, @Model[&quot;Name&quot;], , , ,</td>
</tr>
<tr>
<td>ProcessInjectionTimedOut</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], Config, Process Edited, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], Process was added/edited, @Model.ExternalSeverity, @Model.Data.ProcessFilename, , ,</td>
</tr>
<tr>
<td>ProvisionalEvent</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Process Injection Time Out, @Model[&quot;host&quot;], @Model[&quot;user&quot;], Injection Timeout, @Model.ExternalSeverity, , , , ,</td>
</tr>
<tr>
<td>PublisherChanged</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Threat, Provisional Event, @Model[&quot;host&quot;], @Model[&quot;user&quot;], New provisional event. Prevention Key: @Model[&quot;preventionKey&quot;], @Model.ExternalSeverity, @Model[&quot;EPM&quot;], , , , ,</td>
</tr>
<tr>
<td>QuarantineFailed</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps ESM, @Model[&quot;ProductVersion&quot;], Policy, Trusted Signer Changed, @Model[&quot;esmHost&quot;], @Model[&quot;user&quot;], Hash @Model[&quot;Hash&quot;] trusted signer changed automatically from @Model[&quot;OldPublisher&quot;] to @Model[&quot;NewPublisher&quot;], @Model.ExternalSeverity, @Model[&quot;Hash&quot;], , , , ,</td>
</tr>
<tr>
<td>QuarantineQuotaExceeded</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;], Traps Agent, @Model[&quot;ProductVersion&quot;], Agent, Quarantine Failed, @Model[&quot;host&quot;], @Model[&quot;user&quot;], File @Model[&quot;fileName&quot;] could not be quarantined. Reason: @Model[&quot;FailureReason&quot;], @Model.ExternalSeverity, , , , ,</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>QuarantineSucceeded</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsAgent,@Model[&quot;ProductVersion&quot;],Agent,QuarantineQuota Exceeded,@Model[&quot;host&quot;],@Model[&quot;user&quot;],File@Model[&quot;fileName&quot;] was permanently removed from the quarantine folder because quota was exceeded,@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>ReportingServiceStartFailed</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsAgent,@Model[&quot;ProductVersion&quot;],Agent,QuarantineSucceed,@Model[&quot;host&quot;],@Model[&quot;user&quot;],File@Model[&quot;fileName&quot;] was quarantined successfully,@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>RestoreFailed</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsAgent,@Model[&quot;ProductVersion&quot;],Agent,ReportingService StartFailed,@Model[&quot;host&quot;],@Model[&quot;user&quot;],ReportingService start failed.,@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>RestoreSucceeded</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsAgent,@Model[&quot;ProductVersion&quot;],Agent,RestoreFailed,@Model[&quot;host&quot;],@Model[&quot;user&quot;],File@Model[&quot;fileName&quot;] could not be restored. Reason:@Model[&quot;FailureReason&quot;],@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>RestrictionSettingsEdited</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsAgent,@Model[&quot;ProductVersion&quot;],Agent,RestoreSucceeded,@Model[&quot;host&quot;],@Model[&quot;user&quot;],File@Model[&quot;fileName&quot;] restored successfully,@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>RoleDeleted</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsESM,@Model[&quot;ProductVersion&quot;],Config,RestrictionSettingsEdited,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,Restriction Settings were added/changed,@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>RoleEdited</td>
<td>`&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;]@Model[&quot;EsmIp&quot;] -- @Model[&quot;Time&quot;],TrapsESM,@Model[&quot;ProductVersion&quot;],Config,RoleDeleted,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,Role@Model[&quot;Name&quot;] was deleted,@Model.ExternalSeverity,,,,,,</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RoleStatusChanged</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Config,Role Edited,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,Role @Model.Data.Name was added \changed,@Model.ExternalSeverity,,,,</td>
</tr>
<tr>
<td>RuleDeleted</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Config,Role Status Changed,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,Role @Model[&quot;Name&quot;] status was changed to @Model[&quot;Status&quot;],@Model.ExternalSeverity,,,,</td>
</tr>
<tr>
<td>RuleEdited</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Rule Deleted,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Rule @Model[&quot;id&quot;]: Deleted,@Model.ExternalSeverity,,,@Model[&quot;id&quot;],,,,</td>
</tr>
<tr>
<td>SendingLicenseToClient</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Rule Edited,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Rule @Model.Data.Id: Edited,@Model.ExternalSeverity,,,@Model.Data.Id,,,</td>
</tr>
<tr>
<td>ServerContentRevertFailure</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Config,Sending License To Client,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],@Model[&quot;host&quot;],New license sent,@Model.ExternalSeverity,,,,</td>
</tr>
<tr>
<td>ServerContentRevertSuccess</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Server Content Revert Failure,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Content version failed to revert to @Model[&quot;ContentVersion&quot;]. Error: @Model[&quot;Error&quot;],@Model.ExternalSeverity,,,,,</td>
</tr>
<tr>
<td>ServerContentUpdateFailure</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Server Content Revert Success,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Content version was reverted to @Model[&quot;ContentVersion&quot;] successfully,@Model.ExternalSeverity,,,,,</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServerContentUpdateSuccess</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Server Content Update Failed,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Content version failed to update to @Model[&quot;ContentVersion&quot;]. Error: @Model[&quot;Error&quot;],@Model.ExternalSeverity,,,,,</code></td>
</tr>
<tr>
<td>ServerHeartbeat</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Server Content Update Success,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Content version was updated to @Model[&quot;ContentVersion&quot;] successfully,@Model.ExternalSeverity,,,,,</code></td>
</tr>
<tr>
<td>ServiceAlive</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],System,ESM Heartbeat,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,ESM heartbeat,@Model.ExternalSeverity,,,,,</code></td>
</tr>
<tr>
<td>ServiceStartFailed</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps Agent,@Model[&quot;ProductVersion&quot;],Agent,Service Paused,@Model[&quot;host&quot;],@Model[&quot;user&quot;],Service paused,@Model.ExternalSeverity,,,,,</code></td>
</tr>
<tr>
<td>ServiceStopped</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps Agent,@Model[&quot;ProductVersion&quot;],Agent,Service Start Failed,@Model[&quot;host&quot;],@Model[&quot;user&quot;],Service start failed,@Model.ExternalSeverity,,,,,</code></td>
</tr>
<tr>
<td>ServiceWarning</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps Agent,@Model[&quot;ProductVersion&quot;],Agent,Service Stopped,@Model[&quot;host&quot;],@Model[&quot;user&quot;],Service stopped,@Model.ExternalSeverity,,,,,</code></td>
</tr>
<tr>
<td>SystemShutdown</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps Agent,@Model[&quot;ProductVersion&quot;],Threat,Service Warning,@Model[&quot;host&quot;],@Model[&quot;user&quot;],Warning-Java sandboxed file access to @Model[&quot;TargetValue&quot;],@Model.ExternalSeverity,@Model[&quot;EPM&quot;],,,</code></td>
</tr>
<tr>
<td>TechSupportFileStatus</td>
<td><code>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] - - @Model[&quot;Time&quot;],Traps Agent,@Model[&quot;ProductVersion&quot;],Agent,System</code></td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Shutdown,@Model[&quot;host&quot;],@Model[&quot;user&quot;],Service shutdown,@Model.ExternalSeverity,,,,,</td>
</tr>
<tr>
<td>TrapsServiceStatusChange</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],System,Tech Support File,@Model[&quot;esmHost&quot;],,,, Tech Support File: Status:@Model[&quot;Status&quot;],@Model.ExternalSeverity,,,,,</td>
</tr>
<tr>
<td>UserDeleted</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps Agent,@Model[&quot;ProductVersion&quot;],Agent,Traps Service Status Change,@Model[&quot;host&quot;],@Model[&quot;user&quot;],Agent Service Status Changed: @Model[&quot;OldStatus&quot;] -&gt; @Model[&quot;NewStatus&quot;],@Model.ExternalSeverity,,,,,</td>
</tr>
<tr>
<td>UserEdited</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Config,User Deleted,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,User @Model[&quot;Name&quot;] was deleted.,@Model.ExternalSeverity,,,</td>
</tr>
<tr>
<td>UserLogin</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Config,User Edited,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,User @Model[&quot;Data.Name&quot;] was added \changed.,@Model.ExternalSeverity,,,</td>
</tr>
<tr>
<td>UserStatusChanged</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],System,User Login,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,User @Model[&quot;Data.Username&quot;] logged in to ESM console,@Model.ExternalSeverity,,,</td>
</tr>
<tr>
<td>VerdictChange</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Config,User Status Changed,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],,,User @Model[&quot;Name&quot;] status was changed to @Model[&quot;Status&quot;],@Model.ExternalSeverity,,,</td>
</tr>
<tr>
<td>VerdictChangeAnyToMalware</td>
<td>&lt;134&gt;1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Changed,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict changed. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@@Model[&quot;Hash&quot;],,,</td>
</tr>
<tr>
<td>Event</td>
<td>Syslog Format</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VerdictChangeMalwareToAny</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Changed Any To Malware,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict changed to Malware. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@Model[&quot;Hash&quot;],,,</td>
</tr>
<tr>
<td>VerdictChangeNoConnectionToAny</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Change Malware To Any,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict changed from Malware. Awaiting to restore: @Model[&quot;QuarantineStatus&quot;]. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@Model[&quot;Hash&quot;],,,</td>
</tr>
<tr>
<td>VerdictChangeUnknownToAny</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Change No Connection To Any,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict changed from No Connection. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@Model[&quot;Hash&quot;],,,</td>
</tr>
<tr>
<td>VerdictManualOverride</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Change Unknown To Any,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict changed from Unknown. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@Model[&quot;Hash&quot;],,,</td>
</tr>
<tr>
<td>VerdictRevertedToWildfire</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Manual Override,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict overridden manually. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@Model[&quot;Hash&quot;],,,</td>
</tr>
<tr>
<td>WfCommunicationsStatusChanged</td>
<td><code>&lt;134&gt;</code>1 @Model[&quot;Rfc5424Time&quot;] @Model[&quot;EsmIp&quot;] -- -- @Model[&quot;Time&quot;],Traps ESM,@Model[&quot;ProductVersion&quot;],Policy,Verdict Reverted To Wildfire,@Model[&quot;esmHost&quot;],@Model[&quot;user&quot;],Hash verdict reverted to WildFire. @Model[&quot;OldVerdict&quot;] -&gt; @Model[&quot;NewVerdict&quot;],@Model.ExternalSeverity,@Model[&quot;Hash&quot;],,,</td>
</tr>
</tbody>
</table>
Forward Logs to Email

- Enable Log Forwarding to Email
- Email Format

Enable Log Forwarding to Email

The ESM Console generates logs for over 60 types of events including security events, policy configuration changes, and monitoring events (agent and server). Depending on the type and severity of the data in the log files, you may want to be receive email alerts when critical events require your attention. The ESM Console forwards logs to an email address using the SMTP service. If you want to forward all or some of these logs to an external email address, you can use SSL for reliable and secure transport of logs. After configuring the email reporting settings, you can send a test message to verify the log forwarding settings.

*The date/time of the each logged event is in Universal Time Coordinated (UTC).*

Use the following workflow to configure the ESM Console to send logs and events to an email account.

**STEP 1 |** Enable email reporting.

From the ESM Console, select **Settings > ESM > Email**, and then select **Enable Mail Reporting**.

**STEP 2 |** Configure the email settings.

Specify the following email settings:

- **Display Name**—Display name for the email account that sends the logs.
- **User name**—Name of the user who can access the SMTP service.
- **Password**—Password for the user account that can access the SMTP service.
- **Host**—Hostname or IP address of the SMTP service.
- **Smtp Port**—Communication port of the SMTP service (default is 0).
- **Enable SSL**—Select this option for secure transport of logs in email.
- **Email Address**—Email address of the sender from which the logs are sent.
- **Recipient**—Email address of the recipient to which the logs are sent.
- **Email Timeout (Seconds)**—Period (in seconds) after which the ESM stops trying to send logs (default is 60; range is 1 to 120).

**STEP 3 |** Select the events that you want to send to an external email address.

In the Logging Events area, select one or more of the events. Scroll through the list to see additional types of events you can send.

**STEP 4 |** Save your settings.

Click **Save**.

**STEP 5 |** Verify the configuration of your email settings.

Click **Send Test Message**. The ESM Console sends a test communication to the email address using the information on the Email page. If you do not receive the test message, confirm that your settings are correct and then try again.
### Email Format

The following table lists the events in Email format.

<table>
<thead>
<tr>
<th>Event</th>
<th>Email Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessViolation</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Access Violation&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Target Name:&lt;strong&gt; @Model[&quot;TargetName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>AgentContentUpdate</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent @Model[&quot;host&quot;] received new content version @Model[&quot;ContentVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>AgentPolicyChange</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Policy Change&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ArchivedPreventions</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Archive Threats Events&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Number of Archived Events:&lt;strong&gt; @Model[&quot;totalPreventions&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ArchivedPreventionsFailure</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Archive Threats Events Failed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Number of Archived Events (Actual):&lt;strong&gt; @Model[&quot;progressCount&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Number of Archived Events (Total):&lt;strong&gt; @Model[&quot;totalPreventions&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ClientInstall</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Installed to System&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ClientLicenseInvalid</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent License Invalid&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ClientLicenseRequest</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent License Request&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ClientUninstall</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Uninstalled from System&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ClientUpgrade</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Upgraded&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>CommunicationsCheckWithProxy</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Communications Check With Proxy&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Host:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;ESM Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Status:&lt;strong&gt; @Model[&quot;message&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ConditionDeleted</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Condition Deleted&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Condition Name:&lt;strong&gt; @Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Condition ID:&lt;strong&gt; @Model[&quot;id&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Condition Description:&lt;strong&gt;</code></td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ConditionEdited</td>
<td>@Model[&quot;Description&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ConfigurationChange</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Settings Change&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt; @Model[&quot;Property&quot;] changed from @Model[&quot;OldValue&quot;] to @Model[&quot;NewValue&quot;].&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>DisabledProtection</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Protection Disabled&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt; Protection is disabled across the entire organization!&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>EnabledProtection</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Protection Enabled&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt; Protection is restored across the entire organization!&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>EsmConfigurationChange</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; ESM Configuration Changed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>EsmStatusChange</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; ESM Status Changed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Status:&lt;strong&gt; @Model[&quot;NewStatus&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| LicenseRevoked                          | <html><body><p><div>Log Event:<strong> Agent License Revoked</strong></div><p><div>Time:<strong> @Model.Time (UTC)</strong></div><p><div>Computer:<strong> @Model["host"]</strong></div><p><div>Local Analysis Feature Extraction Failed</strong></div><p><div>Description:<strong> Local Analysis Feature Extraction Failed</strong></div><p><div>Content Version:<strong>@Model["ContentVersion"]</strong></div><p><div>Hash:<strong>@Model["Hash"]</strong></div><p><div>Model Version:<strong>@Model["ContentVersion"]</strong></div><p><div>Server Name:<strong>@Model["esmHost"], @Model["EsmIp"]</strong></div><p><div>By User:<strong>@Model["user"]</strong></div><p><div>Product Version:<strong>@Model["ProductVersion"]</strong></div><p><div>Local Analysis Module Succeeded</strong></div><p><div>Local Analysis Module Version:<strong>@Model["ModuleVersion"]</strong></div><p><div>Local Analysis Module Unavailable</div><p><div>Local Analysis Module Failed</div><p><div>Local Analysis Module Succeeded</p>
<table>
<thead>
<tr>
<th>Event</th>
<th>Email Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>MachineLicenseValidationFailed</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent License Validation Failed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>NewHash</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Hash Added&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Description:&lt;strong&gt; Hash was added to the ESM Hash list&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>NotificationEvent</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Notification Event&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Module Name:&lt;strong&gt; @Model[&quot;EPM&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Process Name:&lt;strong&gt; @Model[&quot;ProcessName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Prevention Key:&lt;strong&gt; @Model[&quot;preventionKey&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Content Version:&lt;strong&gt;@Model[&quot;ContentVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/p&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>OneTimeActionComplete</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent One Time Action Completed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Action Type:&lt;strong&gt; @Model[&quot;ActionType&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Action ID:&lt;strong&gt; @Model[&quot;ActionID&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>OneTimeActionFailed</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent One Time Action Failed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;p&gt;&lt;div&gt;Action Type:&lt;strong&gt; @Model[&quot;ActionType&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ID:&lt;strong&gt; @Model[&quot;ActionID&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
<td>PostDetectionEvent</td>
</tr>
<tr>
<td>PreventionEvent</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Prevention Event&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Module Name:&lt;strong&gt; @Model[&quot;EPM&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Process Name:&lt;strong&gt; @Model[&quot;ProcessName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Prevention Key:&lt;strong&gt; @Model[&quot;preventionKey&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Content Version:&lt;strong&gt;@Model[&quot;ContentVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ProcessCrashed</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Process Crashed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Process name:&lt;strong&gt; @Model[&quot;ProcessName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Error message:&lt;strong&gt; @Model[&quot;message&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ProcessDeleted</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Process Deleted&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Process Name:&lt;strong&gt; @Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ProcessEdited</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Process Added/Edited&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Process Name:&lt;strong&gt; @Model.Data.ProcessFilename&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ProcessInjectionTimedOut</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Process Injection Timeout&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Process Name:&lt;strong&gt; @Model[&quot;ProcessName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;PID:&lt;strong&gt; @Model[&quot;pId&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Severity:&lt;strong&gt; @Model.ExternalSeverity&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ProvisionalEvent</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Provisional Event&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Module Name:&lt;strong&gt; @Model[&quot;EPM&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Process Name:&lt;strong&gt; @Model[&quot;ProcessName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Prevention Key:&lt;strong&gt; @Model[&quot;preventionKey&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Content Version:&lt;strong&gt; @Model[&quot;ContentVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>PublisherChanged</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Trusted Signer changed automatically&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt; Hash trusted signer has changed&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Trusted Signer:&lt;strong&gt; @Model[&quot;OldPublisher&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Trusted Signer:&lt;strong&gt; @Model[&quot;NewPublisher&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>QuarantineFailed</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; File Quarantine Failed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;File Name:&lt;strong&gt; @Model[&quot;fileName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Failure Reason:&lt;strong&gt; @Model[&quot;FailureReason&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt;@Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>QuarantineQuotaExceeded</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Quarantine Quota Exceeded&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;File Name:&lt;strong&gt; @Model[&quot;fileName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>QuarantineSucceeded</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; File Quarantine Succeeded&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;File Name:&lt;strong&gt; @Model[&quot;fileName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt;@Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>ReportingServiceStartFailed</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Reporting Service Start Failed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt;@Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Exception:&lt;strong&gt;@Model[&quot;msg&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>RestoreFailed</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; File Restore Failed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;File Name:&lt;strong&gt; @Model[&quot;fileName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Failure Reason:&lt;strong&gt; @Model[&quot;FailureReason&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt;@Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RestoreSucceeded</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event: &lt;strong&gt;File Restore Succeeded&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time: &lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;File Name: &lt;strong&gt;@Model[&quot;fileName&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer: &lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version: &lt;strong&gt;@Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User: &lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>RestrictionSettingsEdited</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event: &lt;strong&gt;Restrictions Settings Add/Edit&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Description: &lt;strong&gt;Restrictions Settings in the ESM were Added/Edited&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time: &lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User: &lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>RoleDeleted</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event: &lt;strong&gt;Role Deleted&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time: &lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Role Name: &lt;strong&gt;@Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User: &lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>RoleEdited</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event: &lt;strong&gt;Role Added/Edited&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time: &lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Role Name: &lt;strong&gt;@Model.Data.Name&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User: &lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>RoleStatusChanged</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event: &lt;strong&gt;Role Status Changed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time: &lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Role Name: &lt;strong&gt;@Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Status: &lt;strong&gt;@Model[&quot;Status&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User: &lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>RuleDeleted</td>
<td><code>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event: &lt;strong&gt;Rule Deleted&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time: &lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Rule Name: &lt;strong&gt;@Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Rule ID: &lt;strong&gt;@Model[&quot;id&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User: &lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</code></td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>strong&gt;&lt;/div&gt;&lt;div&gt;Rule Description:&lt;strong&gt; @Model[&quot;Description&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>RuleEdited</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;Log Event:&lt;strong&gt; Rule Added/Edited&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Rule Name:&lt;strong&gt; @Model.Data.Name&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Rule ID:&lt;strong&gt; @Model.Data.Id&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Rule Description:&lt;strong&gt; @Model.Data.Description&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>SendingLicenseToClient</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;Log Event:&lt;strong&gt; License Sent to Agent&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServerContentRevertFailure</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;Log Event:&lt;strong&gt; Content version failed to revert to @Model[&quot;ContentVersion&quot;]. Error: @Model[&quot;Error&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServerContentRevertSuccess</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;Log Event:&lt;strong&gt; Content version was reverted to @Model[&quot;ContentVersion&quot;] successfully.&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServerContentUpdateFailure</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;Log Event:&lt;strong&gt; Content version failed to update to @Model[&quot;ContentVersion&quot;]. Error: @Model[&quot;Error&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
</tbody>
</table>
| ServerContentUpdateSuccess| &lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;/div&gt;&lt;div&gt;Log Event:&lt;strong&gt; Content version was updated to @Model["ContentVersion"] successfully.&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;
<table>
<thead>
<tr>
<th>Event</th>
<th>Email Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerHeartbeat</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; ESM Heartbeat&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServiceAlive</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Service Start&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServiceStartFailed</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Service Start Failed&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Error:&lt;strong&gt; @Model[&quot;Error&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServiceStopped</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Service Stopped&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>ServiceWarning</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Service Warning&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Java sandbox file access to:&lt;strong&gt; @Model[&quot;TargetValue&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>SystemShutdown</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Agent Shutdown&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt; @Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TechSupportFileStatus</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt;Tech Support File&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Description:&lt;strong&gt;Tech Support File Generation&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Time:&lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Job:&lt;strong&gt;@Model[&quot;JobID&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Status:&lt;strong&gt;@Model[&quot;Status&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt;@Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>TrapsServiceStatusChange</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt;Agent Service Status Changed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Computer:&lt;strong&gt;@Model[&quot;host&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Agent Version:&lt;strong&gt;@Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Status:&lt;strong&gt;@Model[&quot;OldStatus&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Status:&lt;strong&gt;@Model[&quot;NewStatus&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>UserDeleted</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt;User Deleted&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Deleted User Name:&lt;strong&gt;@Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>UserEdited</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt;User Added/Edited&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Added/Edited User Name:&lt;strong&gt;@Model.Data.Name&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>UserLogin</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt;User Login&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;User:&lt;strong&gt;@Model.Data.Username&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>UserStatusChanged</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt;User Status Changed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;div&gt;Time:&lt;strong&gt;@Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;User Name:&lt;strong&gt;@Model[&quot;Name&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Status:&lt;strong&gt;@Model[&quot;Status&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>-------</td>
<td>--------------</td>
</tr>
<tr>
<td>VerdictChange</td>
<td>User:&lt;strong&gt;@Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt;Hash Verdict has Changed&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt;@Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt;@Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>VerdictChangeAnyToMalware</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Verdict Changed - Any to Malware&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt;Hash Verdict has Changed to Malware&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt;@Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt;@Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>VerdictChangeMalwareToAny</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Verdict Changed - Malware to Any&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt;Hash Verdict has Changed from Malware.&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Awaiting to restore:&lt;strong&gt;@Model[&quot;QuarantineStatus&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt;@Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt;@Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>VerdictChangeNoConnectionToAny</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Verdict Changed - No connection to Any&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt;Hash Verdict has Changed from No connection&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt;@Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt;@Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>VerdictChangeUnknownToAny</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Verdict Changed - Unknown to Any&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt;Hash Verdict has Changed from Unknown&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt;@Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt;@Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>Event</td>
<td>Email Format</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VerdictManualOverride</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Verdict Manual Override&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt; Hash verdict overridden manually&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt; @Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt; @Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>VerdictRevertedToWildfire</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; Verdict Reverted To WildFire&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Description:&lt;strong&gt; Hash Verdict reverted to WildFire&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Hash:&lt;strong&gt; @Model[&quot;Hash&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Previous Verdict:&lt;strong&gt; @Model[&quot;OldVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;New Verdict:&lt;strong&gt; @Model[&quot;NewVerdict&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;By User:&lt;strong&gt; @Model[&quot;user&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td>WfCommunicationsStatusChanged</td>
<td>&lt;html&gt;&lt;body&gt;&lt;p&gt;&lt;div&gt;Log Event:&lt;strong&gt; WildFire Communications Status Changed&lt;/strong&gt;&lt;/div&gt;&lt;p&gt;&lt;/p&gt;&lt;div&gt;Time:&lt;strong&gt; @Model.Time (UTC)&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Server Name:&lt;strong&gt; @Model[&quot;esmHost&quot;], @Model[&quot;EsmIp&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;ESM Version:&lt;strong&gt; @Model[&quot;ProductVersion&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;div&gt;Status:&lt;strong&gt; @Model[&quot;message&quot;]&lt;/strong&gt;&lt;/div&gt;&lt;/p&gt;&lt;/body&gt;&lt;/html&gt;</td>
</tr>
</tbody>
</table>
Troubleshooting

> Traps Troubleshooting Resources
> Traps and Endpoint Security Manager Processes
> ESM Tech Support File
> Database (DB) Configuration Tool
> Cytool
> Troubleshoot Traps Issues
> Troubleshoot ESM Console Issues
Traps Troubleshooting Resources

To troubleshoot Traps and the Endpoint Security Manager (comprising an ESM Server, the ESM Console, and a database), use the following resources:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESM Resources</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Endpoint Security Manager</strong></td>
<td>Web interface, which provides reports and logs. The information is useful for monitoring and filtering the logs to interpret unusual behavior on your network. After analyzing a security event, you can choose to create a custom rule for the endpoint or process.</td>
</tr>
<tr>
<td><strong>DebugWeb log</strong></td>
<td>Indicates information, warnings, and errors related to the Endpoint Security Manager. The DebugWeb log is located in the %ProgramData%\Cyvera\Logs folder of the ESM Server.</td>
</tr>
<tr>
<td><strong>Server log</strong></td>
<td>Indicates information, warnings, and errors related to the Endpoint Database and ESM Server. The Server log is located in the %ProgramData%\Cyvera\Logs folder of the ESM Server.</td>
</tr>
<tr>
<td><strong>ESM installation log</strong></td>
<td>Specifies any errors encountered during installation of ESM components. Use this log file when you need to troubleshoot installation issues. The installer stores the log files in the %temp% or C:\Users&lt;user_name&gt;\AppData\Local\Temp folder.</td>
</tr>
<tr>
<td><strong>Database (DB) Configuration Tool (dbconfig.exe)</strong></td>
<td>Command-line interface that provides an alternative to managing basic server settings using the ESM Console. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt run as an administrator. For more information, see Database (DB) Configuration Tool.</td>
</tr>
<tr>
<td><strong>ESM Tech Support file</strong></td>
<td>On-demand aggregation of active ESM Console and ESM Server logs and settings to aid Technical Support in troubleshooting and diagnosing issues. For more information, see ESM Tech Support File.</td>
</tr>
<tr>
<td><strong>Traps Resources</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Traps installation log</strong></td>
<td>Specifies any errors encountered during installation of Traps. Use this log file when you need to troubleshoot installation issues. The installer stores the log files in the %temp% or C:\Users&lt;user_name&gt;\AppData\Local\Temp folder.</td>
</tr>
<tr>
<td><strong>Traps service log</strong></td>
<td>Indicates information, warnings, and errors related to the Traps service. The Service log is located in the following folder on the endpoint:</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista and later: %ProgramData%\Cyvera\Logs</td>
</tr>
<tr>
<td></td>
<td>• Windows XP: C:\Document and Settings\All Users\Application Data\Cyvera\Logs</td>
</tr>
<tr>
<td><strong>Traps console log</strong></td>
<td>Indicates information, warnings, and errors related to the Traps console. The Console log is located in the following folder on the endpoint:</td>
</tr>
<tr>
<td>Resource</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Windows Vista and later: C:\Users&lt;username&gt;\AppData\Roaming\Cyvera</td>
<td></td>
</tr>
<tr>
<td>• Windows XP: C:\Document and Settings&lt;username&gt;\Application Data\Cyvera\Logs</td>
<td></td>
</tr>
<tr>
<td>Traps and ESM initiated processes</td>
<td>See Traps and Endpoint Security Manager Processes.</td>
</tr>
<tr>
<td>Supervisor Command Line Tool (cytool.exe)</td>
<td>Allows you to enumerate protected processes, enable or disable protection</td>
</tr>
<tr>
<td></td>
<td>features, and enable or disable Traps management actions from a command</td>
</tr>
<tr>
<td></td>
<td>line interface. For more information, see Cytool.</td>
</tr>
<tr>
<td>Unknown files for analysis</td>
<td>Traps stores unknown files to send to the ESM Server in the C:\ProgramData\Cyvera\Temp folder. After the ESM Server submits a file to WildFire, the Traps agent deletes the file from the Temp folder. In some cases, third-party Antivirus (AV) applications can raise an alert for this folder. If this occurs, it is recommended to whitelist this folder in the third-party AV application.</td>
</tr>
</tbody>
</table>
## Traps and Endpoint Security Manager Processes

The following processes are initiated by Traps and the Endpoint Security Manager (ESM).

<table>
<thead>
<tr>
<th>Component</th>
<th>Process Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps agent</td>
<td>CyveraConsole.exe</td>
<td>User interface for the Traps console. Runs only after the user launches the console from the notification area (system tray).</td>
</tr>
<tr>
<td>Traps agent</td>
<td>CyveraService.exe</td>
<td>Traps agent core service, which works with Cyserver.exe to enforce the policy, communicate with the server, and prevent security attacks, when needed.</td>
</tr>
<tr>
<td>Traps agent</td>
<td>Cyserver.exe</td>
<td>Traps agent core service, which works with CyveraService.exe to enforce the policy, communicate with the server, and prevent security attacks, when needed.</td>
</tr>
<tr>
<td>Traps agent</td>
<td>Cytray.exe</td>
<td>Traps Tray process, allows the user to click on the tray icon and run the console. Runs constantly in the background.</td>
</tr>
<tr>
<td>Traps agent</td>
<td>Tda.exe</td>
<td>Traps dump analyzer, which analyzes the contents of memory locations and other data when a prevention event occurs on the endpoint.</td>
</tr>
<tr>
<td>Traps agent</td>
<td>Tdawork.exe</td>
<td>Traps dump analyzer worker processes, one per processor. These processes run in the background and should run constantly.</td>
</tr>
<tr>
<td>ESM Server</td>
<td>CyveraServer.exe</td>
<td>ESM Server core service, which communicates with the agents and with WildFire.</td>
</tr>
</tbody>
</table>
ESM Tech Support File

From the ESM Console, you can create an ESM tech support file containing the following information:

- Effective security policy
- ESM Console and ESM Server settings
- ESM Console and ESM Server logs
- Database query results

The ESM Console aggregates and packages these logs into a ZIP file (< 1GB) that you can then download and send to Technical Support. Each time you generate a new ESM tech support file, the ESM Console logs the event. You can view the status and history of all tech support files from the ESM Console and can also configure log forwarding to send logs about the status of ESM tech support files to an external logging platform or to an email address.

You can generate an ESM tech support file from the Settings page. On average, this process takes 10 minutes or fewer.

**STEP 1 |** From the ESM Console, select **Settings**.

**STEP 2 |** Select **Generate** to start the collection process. The ESM Console deactivates (grays out) the **Generate** button during generation process.

**STEP 3 |** Refresh the page to view the status of the file. When the file is available, the ESM Console displays the time the file was created and updates the file size in the download link. The ESM Console reports a failure if it fails to generate the file within the preconfigured timeout period (25 minutes).

You can also monitor logs related to ESM tech support file generation on the **Monitor > ESM > Logs** page. From there, you can filter the Report Type by Tech Support File Status, or filter the Message by a specific job ID.

**STEP 4 |** Click **Download** to save the file and then send it to Technical Support, as needed. To view the history of all available ESM tech support file requests, select **Monitor > Data Retrieval** page. From there, you can download previous files or delete them as needed. If the tech support file failed to generate, the **Download** button is hidden and you can only **Delete** the request.
Database (DB) Configuration Tool

The DB Configuration Tool is a command-line interface that provides an alternative to managing basic server settings using the ESM Console. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt run as an administrator. The DB Configuration Tool is located in the Server folder of the Endpoint Security Manager (ESM) Server.

Use the DB Configuration Tool to perform the following functions:

- **Access the Database Configuration Tool**
- **Configure Administrative Access to the ESM Console Using the DB Configuration Tool**
- **Configure ESM Server Settings Using the DB Configuration Tool**
- **Customizable ESM Server Settings**
- **Change the Ninja-Mode Password**
- **Enable Log Forwarding to an External Logging Platform Using the DB Configuration Tool**

Access the Database Configuration Tool

Run the DB Configuration Tool from the Server folder on an ESM Server to view syntax and usage examples.

> All commands run using the DB Configuration Tool are case sensitive.

**STEP 1** | Open a command prompt as an administrator:
- Select Start > All Programs > Accessories. Right-click Command prompt, and then select Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

**STEP 2** | Navigate to the folder that contains the DB Configuration Tool:

C:\Users\Administrator> cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server

**STEP 3** | View usage and options for the DB Configuration Tool:

c:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig
Usage:
> DBConfig.exe importLicense [1]
Add a new license to the database.
1) CyveraLicense.xml full path
> DBConfig.exe [1] [2] [3]
Write a configuration to the database.
1) Configuration Type (Server, Reflector, UserManagement, Reporting)
2) Key Name
3) Value
> DBConfig.exe [1] show
Show the values of a specific configuration.
1) Configuration Type (Server, Reflector, UserManagement, Reporting)
Examples:
Configure Administrative Access to the ESM Console Using the DB Configuration Tool

When you install the ESM Console, you specify the administrative account and type of authentication (machine or domain) that you will use for initial access to the ESM Console. From the ESM Console, you can then configure role-based access control to define Administrative Roles to assign to Administrative Users (and/or groups). This enables you to enforce the separation of information among functional or regional areas of your organization to protect the privacy of data on the ESM Console. For more information, see Manage Administrator Access to the ESM Console.

If after setting up role-based access you have difficulty accessing the ESM Console and need to verify or change administrative account settings, you can use a command line interface (CLI) called the DB Configuration Tool. This allows you to manage basic ESM Console settings including the administrative users that have access to the ESM Console, and the authentication mode by which to authenticate them. The DB Configuration Tool does not validate or authenticate the users and only provides a mechanism for making changes when you cannot do so using the ESM Console.

To enforce role-based access control, use the ESM Console to make changes to administrative access, when possible.

You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt that you run as an administrator. The DB Configuration Tool is located in the `Server` folder on the ESM Server.

All commands you run using the DB Configuration Tool are case sensitive.

**STEP 1** | Open a command prompt as an administrator in either of two ways:
- Select Start > All Programs > Accessories, right-click Command prompt, and then select Run as administrator.
- Select Start and, in the Start Search box, type cmd but do not press Enter, yet. Then, to open the command prompt as an administrator, press Ctrl+Shift+Enter.

**STEP 2** | Navigate to the folder that contains the DB Configuration Tool:

```
C:\Users\Administrator> cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server
```

**STEP 3** | (Optional) View the existing administrator settings:

```
C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig usermanagement show
AuthMode = Machine
AllowedUsers = Administrator
AllowedGroups =
```

**STEP 4** | (Optional) Specify the authentication mode: either domain or machine.
Configure ESM Server Settings Using the DB Configuration Tool

The DB Configuration Tool is a command-line interface (CLI) that provides an alternative to managing basic server settings through the ESM Console. Examples of settings that you can change include the ninja mode password, active directory caching, and number of logs included in the ESM Tech Support file. For the full list, see Customizable ESM Server Settings.

You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt that you run as an administrator. The DB Configuration Tool is located in the Server folder on the ESM Server.

All commands you run using the DB Configuration Tool are case sensitive.

STEP 1 | Open a command prompt as an administrator in either of two ways:

- Select Start > All Programs > Accessories. Right-click Command prompt, and then select Run as administrator.
- Select Start and, in the Start Search box, type cmd but do not press Enter, yet. Then, to open the CLI command window as an administrator, press Ctrl+Shift+Enter.

STEP 2 | Navigate to the folder that contains the DB Configuration Tool:

C:\Users\Administrator> cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server

STEP 3 | View the existing server settings:

C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server show
PreventionsDestFolder =
InventoryInterval = 284
HeartBeatGracePeriod = 4200
NinjaModePassword = Password2
BitsUrl = http://CYVERASERVER:80/BitsUploads
MaxActions = 1000
BitsUploadTimeoutInterval = 360
BitsUploadTimeout = 720
KeepAliveTimeout = 0

C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig usermanagement AuthMode [domain|machine]

STEP 5 | (Optional) Add an administrative user.

C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig usermanagement AllowedUsers <newuser>

Repeat this step to add additional administrative users. The DB Configuration Tool appends the usernames to the existing list of administrative users.

To remove administrative users, you must use the ESM Console.
STEP 4 | (Optional) Configure or change any of the ESM Server settings, as needed. For usage guidelines and default values, see Customizable ESM Server Settings. For example, to specify the allowable grace period, in seconds, for an endpoint that is not responding (range is 300 to 86,400; default is 4200):

C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server> dbconfig server HeartBeatGracePeriod <value>

For example, a value of 300 means that if the ESM Server does not receive any communication from the endpoint within five minutes (300 seconds), the Endpoint Security Manager reports the endpoint status as disconnected.

Customizable ESM Server Settings

The following table lists the settings that you can configure for the ESM Server.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreventionsDestFolder = &lt;folder&gt;</td>
<td>Legacy upload network location (required for Traps 3.1 and earlier agents).</td>
<td>N/A</td>
</tr>
<tr>
<td>InventoryInterval = &lt;hours&gt;</td>
<td>Frequency at which Traps sends the list of applications running on the endpoint to the ESM Server.</td>
<td>284; range 1 to 14400</td>
</tr>
<tr>
<td>HeartBeatGracePeriod = &lt;seconds&gt;</td>
<td>Period of no communication between the Traps agent and the ESM Server after which, the Endpoint Security Manager reports the endpoint status as disconnected.</td>
<td>4200; range is 300 to 86400</td>
</tr>
<tr>
<td>NinjaModePassword = &lt;password&gt;</td>
<td>Password required to access configuration settings that are available in ninja mode on the ESM Console.</td>
<td>Password2</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td><code>BitsUrl = &lt;url&gt;</code></td>
<td>URL of the BITS server to which the agent uploads forensic data, for example <a href="http://ESMSERVER:80/BitsUploads">http://ESMSERVER:80/BitsUploads</a>.</td>
<td>N/A</td>
</tr>
<tr>
<td><code>MaxActions = &lt;totalnumber&gt;</code></td>
<td>Maximum number of actions the ESM Server can send in a single call to an agent.</td>
<td>1000; range is 1 to 2147483647</td>
</tr>
<tr>
<td><code>BitsUploadTimeoutInterval = &lt;minutes&gt;</code></td>
<td>Interval at which the Traps agent retries to upload data to the BITS server.</td>
<td>360; range is 1 to 2000</td>
</tr>
<tr>
<td><code>BitsUploadTimeout = &lt;minutes&gt;</code></td>
<td>Period after which the Traps agent stops trying to upload data to the BITS folder. After this period, the upload state changes from in progress to failed.</td>
<td>720; range is 1 to 2000</td>
</tr>
<tr>
<td><code>KeepAliveTimeout = &lt;seconds&gt;</code></td>
<td>Interval at which the ESM Server sends keep-alive messages to the SIEM. A value of 0 indicates the ESM Server will not send messages.</td>
<td>0; range is 0 to 2147483647</td>
</tr>
<tr>
<td><code>ExternalAddress = &lt;url&gt;</code></td>
<td>Changes the URL of the external BITS server address for the specific ESM Server on which you run the command. This field is used in deployments with multiple ESM Servers.</td>
<td>N/A</td>
</tr>
<tr>
<td><code>VdiHeartbeatGracePeriod = &lt;minutes&gt;</code></td>
<td>Period after which the ESM Console detaches a license for a disconnected VDI session to free it up for reuse.</td>
<td>25; range is 1 to 120</td>
</tr>
<tr>
<td>`UseDnsForAddressResolution = [True</td>
<td>False]`</td>
<td>Use DNS for address resolution if the agent does not send the address.</td>
</tr>
<tr>
<td><code>TaskTimeout = &lt;minutes&gt;</code></td>
<td>The period of time at which the status of a scheduled task changes from in progress to failed.</td>
<td>30; range is 0 to 2147483647</td>
</tr>
<tr>
<td><code>SqlDateTimeFormat</code></td>
<td>Not used.</td>
<td>N/A</td>
</tr>
<tr>
<td><code>TaskOverrideInMinutes = &lt;minutes&gt;</code></td>
<td>The period of time at which the status of a scheduled buffer processing task changes from in progress to failed.</td>
<td>30</td>
</tr>
<tr>
<td>`EnableStatistics = [True</td>
<td>False]`</td>
<td>Enables tracking of real-time performance counters between the agent, ESM Server, and WildFire. To view the statistics of communication requests that succeed or fail, use the Windows Performance</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>ActiveDirectoryPathUpdateInterval= &lt;minutes&gt;</strong></td>
<td>Interval at which the ESM Server updates the Active Directory machine path.</td>
<td>1440</td>
</tr>
<tr>
<td><strong>ActiveDirectoryGroupsUpdateInterval= &lt;minutes&gt;</strong></td>
<td>Interval at which the ESM Server updates the Active Directory group members.</td>
<td>1440</td>
</tr>
<tr>
<td>**EnableADCache = [True</td>
<td>False]**</td>
<td>Enable Active Directory caching. When this is set to False, the ESM Console queries Active Directory on every agent heartbeat for every Active Directory target object.</td>
</tr>
<tr>
<td><strong>ContentVersion = &lt;version&gt;</strong></td>
<td>Reserved for internal use.</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>ContentUpdateTimeoutMinutes = &lt;minutes&gt;</strong></td>
<td>The period of time after which a content update reports an error if installation fails.</td>
<td>30</td>
</tr>
<tr>
<td><strong>SupportFileCollectionTimeout = &lt;minutes&gt;</strong></td>
<td>The period of time in which the ESM Console must finish collecting logs for the ESM Tech Support file.</td>
<td>10</td>
</tr>
<tr>
<td><strong>SupportFileAggregationTimeout = &lt;minutes&gt;</strong></td>
<td>The period of time in which the ESM Console must finish aggregating logs for the ESM Tech Support file. After this period, the status changes from in progress to failed.</td>
<td>20</td>
</tr>
<tr>
<td><strong>MaxCollectedIisLogs = &lt;iislogs&gt;</strong></td>
<td>The maximum number of collected IIS logs the ESM Console collects when creating the ESM Tech Support file.</td>
<td>100</td>
</tr>
<tr>
<td><strong>MaxCollectedNlogLogs = &lt;nlogs&gt;</strong></td>
<td>The maximum number of collected server logs the ESM Console collects when creating the ESM Tech Support file.</td>
<td>1000</td>
</tr>
<tr>
<td><strong>MaxCollectedDbRows = &lt;dbrows&gt;</strong></td>
<td>The maximum number of database records the ESM Console collects when creating the ESM Tech Support file.</td>
<td>100000</td>
</tr>
<tr>
<td>**UseContentProductionKey = [True</td>
<td>False]**</td>
<td>When set to True, the ESM Console uses only production content packages.</td>
</tr>
</tbody>
</table>
Cytool

Cytool is a command-line interface that is integrated into Traps that enables you to query and manage basic functions of Traps. Changes made using Cytool are active until Traps receives the next heartbeat communication from the ESM Server.

You can access the Cytool using a Microsoft MS-DOS command prompt run as an administrator. Cytool is located in the Traps folder on the Endpoint.

Use Cytool to perform the following functions:

- Access Cytool
- View Processes Currently Protected by Traps Using Cytool
- Manage Protection Settings on the Endpoint Using Cytool
- Manage Traps Drivers and Services on the Endpoint Using Cytool
- View and Compare Security Policies on an Endpoint Using Cytool
- Manage Logging of Traps Components Using Cytool
- Restore a Quarantined File Using Cytool
- View Statistics for a Protected Process Using Cytool
- View Details About the Traps Local Analysis Module Using Cytool
- View Hash Details About a File Using Cytool

Access Cytool

To view syntax and usage examples for Cytool commands, use the /? option after any command.

**STEP 1** | Open a command prompt as an administrator:

- Select Start > All Programs > Accessories. Right-click Command prompt, and then select Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

**STEP 2** | Navigate to the folder that contains Cytool:

C:\Users\Administrator> cd C:\Program Files\Palo Alto Networks\Traps

**STEP 3** | View usage and options for the Cytool command:

c:\Program Files\Palo Alto Networks\Traps> cytool /?
Traps (R) supervisor tool 3.1
(c) Palo Alto Networks, Inc. All rights reserved
Usage: CYTOOL [/?] [/a] [command [options]]
Options:
/? Display this help message.
/a Authenticate as supervisor.
command enum | protect | startup | runtime | policy
For more information on a specific command run CYTOOL command /?
View Processes Currently Protected by Traps Using Cytool

To view processes that Traps is currently injected into, run the `enum` command using Cytool or view the Protection tab on the Traps Console (see View Processes Currently Protected by Traps). By default, both the Traps Console and Cytool display only the protected processes run by the current user. To view protected processes run by all users, specify the `/a` option.

Viewing protected processes run by all users requires you to enter the supervisor (uninstall) password.

**STEP 1** | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2** | View protected processes initiated by the current user by entering the `cytool enum` command. To view protected processes for all users on the endpoint, specify the `/a` option, and enter the supervisor password when prompted.

```
c:\Program Files\Palo Alto Networks\Traps> cytool /a enum
Enter supervisor password:
Process ID     Agent Version
  1000 3.1.1546
  1468 3.1.1546
   452 3.1.1546
   [...]
```

Manage Protection Settings on the Endpoint Using Cytool

By default, Traps protects core processes, registry keys, Traps files, and Traps services according to the service protection rules defined in the security policy (for information about configuring service protection rules in the Endpoint Security Manager, see Manage Service Protection). You can use Cytool to override the security rules and manage the following layers of protection that Traps applies on the endpoint:

- Enable or Disable Core Process Protection on the Endpoint
- Enable or Disable Registry Protection Settings on the Endpoint
- Enable or Disable Traps File Protection Settings on the Endpoint
- Enable or Disable Service Protection Settings on the Endpoint
- Use the Security Policy to Manage Service Protection

**Enable or Disable Core Process Protection on the Endpoint**

By default, Traps protects core processes including Cyserver.exe and CyveraService.exe based on the service protection rules defined in the local security policy. If required, you can override the behavior of core process protection using the `cytool protect [enable|disable] process` command.

Changing the protection settings requires you to enter the supervisor (uninstall password).

**STEP 1** | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2** | To manage the protection settings of core processes on the endpoint, use the following command:

```
c:\Program Files\Palo Alto Networks\Traps> cytool protect [enable|disable] process
```
The following example displays output for enabling protection of core processes. The Mode column displays the revised protection status, either Enabled or Disabled, or Policy when using the settings in the local security policy to protect core processes.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable process
Enter supervisor password:
Protection Mode State
Process Enabled Enabled
Registry Policy Disabled
File Policy Disabled
Service Policy Disabled
```

To use the default policy rule settings to protect core processes on the endpoint, see Use the Security Policy to Manage Service Protection.

**Enable or Disable Registry Protection Settings on the Endpoint**

To prevent attackers from tampering with the Traps registry keys, use the `cytool protect enable registry` command to restrict access to the registry keys stored in HKLM\SYSTEM\Cyvera. To disable protection of the registry keys, use the `cytool protect disable registry` command.

Making changes to the registry protection settings requires you to enter the supervisor (uninstall) password when prompted.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2 |** To manage the protection settings of registry keys on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect [enable|disable] registry
```

The following example displays output for enabling protection of registry keys. The Mode column displays the revised protection status, either Enabled or Disabled, or Policy when using the settings in the local security policy to protect registry keys.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable registry
Enter supervisor password:
Protection Mode State
Process Policy Disabled
Registry Enabled Enabled
File Policy Disabled
Service Policy Disabled
```

To use the settings in the local security policy to protect registry keys on the endpoint, see Use the Security Policy to Manage Service Protection.

**Enable or Disable Traps File Protection Settings on the Endpoint**

To prevent attackers from tampering with the Traps files, use the `cytool protect enable file` command to restrict access to the system files stored in %Program Files%\Palo Alto Networks\Traps and %ProgramData%\Cyvera (or C: \ Documents and Settings\All Users
To disable protection of Traps files, use the `cytool protect disable file` command.

Making changes to the Traps file protection settings requires you to enter the supervisor (uninstall) password when prompted.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2 |** To manage the protection settings of Traps files on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool protect [enable|disable] file
```

The following example displays output for enabling protection of files. The `Mode` column displays the revised protection status, either Enabled or Disabled, or Policy when using the settings in the local security policy to protect Traps files.

```
C:\Program Files\Palo Alto Networks\Traps> cytool protect enable file
Enter supervisor password:
Protection Mode State
Process Policy Disabled
Registry Policy Disabled
File Enabled Enabled
Service Policy Disabled
```

To use the default policy rule settings to protect Traps files on the endpoint, see Use the Security Policy to Manage Service Protection.

### Enable or Disable Service Protection Settings on the Endpoint

To bypass the Traps security policy, attackers can attempt to disable or change the status of Traps services. Use the `cytool protect enable service` command to protect Traps services. To disable protection of Traps services, use the `cytool protect disable service` command.

Making changes to the service protection settings requires you to enter the supervisor (uninstall) password when prompted.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2 |** To manage the protection settings of Traps services on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool protect [enable|disable] service
```

The following example displays output for enabling protection of services. The `Mode` column displays the revised protection status, either Enabled or Disabled, or Policy when Traps uses the settings in the local security policy to protect Traps services.

```
C:\Program Files\Palo Alto Networks\Traps> cytool protect enable service
Enter supervisor password:
Protection Mode State
Process Policy Disabled
```
To use the default policy rule settings to protect Traps services on the endpoint, see Use the Security Policy to Manage Service Protection.

Use the Security Policy to Manage Service Protection

After changing protection settings using Cytool, you can restore the default security policy at any time using the `cytool protect policy <feature>` command.

STEP 1 | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

STEP 2 | To use the rules in the security policy to manage service protection, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool protect policy <feature>
```

where `<feature>` is either `process`, `registry`, `file`, or `service`.

The following example displays output for managing the protection on Traps files using the local security policy. The `Mode` column displays the revised protection status as `Policy`.

```
C:\Program Files\Palo Alto Networks\Traps> cytool protect policy <feature>
Enter supervisor password:
Protection Mode State
Process Enabled Enabled
Registry Enabled Enabled
File Policy Disabled
Service Enabled Enabled
```

Manage Traps Drivers and Services on the Endpoint Using Cytool

When an endpoint boots, Traps starts drivers (Cyverak, Cyvrmtgn, and Cyvrfsfd) and services (Cyvera and CyveraService) by default. You can use Cytool to override the default behavior and manage the startup or current status of drivers and services on a global or individual basis. Changes to the default startup behavior take effect when the endpoint restarts. Changes to the runtime behavior take immediate effect.

- View Traps Startup Components on the Endpoint
- Enable or Disable the Startup of Traps Components on the Endpoint
- View Traps Runtime Components on the Endpoint
- Start or Stop Traps Runtime Components on the Endpoint

View Traps Startup Components on the Endpoint

Use the `cytool startup query` command to view the status of startup components on the endpoint. When a service or driver is disabled, Cytool displays the component as `Disabled`. When a driver is enabled, Cytool displays the component as `System`. When a service is enabled, Cytool displays the component `Startup` as `Automatic`.

STEP 1 | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).
STEP 2 | To view the current startup behavior of Traps drivers and services, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool startup query
Service Startup
cyverak System
cyvrmtgn System
cyvrfsfd System
cyserver Automatic
CyveraService Automatic
```

Enable or Disable the Startup of Traps Components on the Endpoint

Use the `cytool startup [enable|disable]` command optionally followed by the component name to override the default behavior for starting Traps drivers and services on and endpoint.

Making changes to the startup behavior requires you to enter the supervisor password when prompted.

Changes to Traps drivers and services do not take effect until the system restarts. To make changes to Traps drivers and services that take effect immediately, see Start or Stop Traps Runtime Components on the Endpoint.

STEP 1 | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

STEP 2 | To change the startup behavior for a specific driver or service, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool startup [enable|disable] <component>
```

where `<component>` is either a driver: `cyverak, cyvrmtgn, cyvrfsfd`; or a service: `cyserver, CyveraService`.

Alternatively, you can omit `<component>` from the command to change the startup behavior for all drivers and services.

The following example displays output for disabling the startup behavior of the cyvrmtgn driver. The `Startup` column displays the revised behavior as `Disabled`.

```
C:\Program Files\Palo Alto Networks\Traps> cytool startup disable cyvrmtgn
Enter supervisor password:
Service Startup
cyverak System
cyvrmtgn Disabled
cyvrfsfd System
cyserver Automatic
CyveraService Automatic
```

View Traps Runtime Components on the Endpoint

Use the `cytool runtime query` command to view the status of Traps components on the endpoint. When a service or driver is active, Cytool displays the state as `Running`. When a service or driver is not running, Cytool displays the state as `Stopped`.

STEP 1 | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).
STEP 2 | To view the current runtime state of Traps drivers and services, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool runtime query
```

Enter supervisor password:

Service Startup
- cyverak Running
- cyvrmtgn Running
- cyvrfsfd Running
- cyserver Stopped
- CyveraService Running

**Start or Stop Traps Runtime Components on the Endpoint**

In situations where the Traps agent cannot reach the ESM Server or you do not have permission to change the behavior of Traps from the ESM Console but must solve an urgent issue related to Traps drivers and services, you can use the `cytool runtime [start|stop]` command to override the default runtime behavior. The command is useful when you must take immediate action to start or stop all Traps components or start or stop a specific Traps driver or service.

Changes to the runtime behavior of Traps drivers and services reset when the system restarts. To make changes to the startup behavior of Traps drivers and services, see [Enable or Disable the Startup of Traps Components on the Endpoint](#).

Making changes to the runtime behavior requires you to enter the supervisor (uninstall) password when prompted.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2 |** To start or stop a driver or service, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool runtime start <component>
```

where `<component>` is either a driver: `cyverak, cyvrmtgn, cyvrfsfd`; or a service: `cyserver, CyveraService`.

Alternatively, you can omit `<component>` from the command to change the runtime behavior for all drivers and services.

The following example displays output for stopping the `cyserver` service. The **Startup** column displays the revised component status, either **Running** or **Stopped**.

```
C:\Program Files\Palo Alto Networks\Traps> cytool runtime stop cyserver
Enter supervisor password:
Service Startup
- cyverak Running
- cyvrmtgn Running
- cyvrfsfd Running
- cyserver Stopped
- CyveraService Running
```
View and Compare Security Policies on an Endpoint Using Cytool

Using Cytool, you can display details about security policies on the endpoint.

- View Details About an Active Policy
- Compare Policies

**View Details About an Active Policy**

Use the `cytool policy query <process>` command to view details about policies associated with a specific process. Specifying the process name displays details about the intended policy whereas specifying the process ID (PID) displays details about the active policy that is currently applied to the process. The output is helpful when you want to verify that a policy is implemented in the way you intended to configure it.

To view policy details, you must enter the supervisor (uninstall) password when prompted.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2 |** To view the active policy for a process, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool policy query <process>
```

where `<process>` is either the process name or PID. For example, to view details about a policy for notepad, enter `cytool policy query notepad`. The following example displays policy details for a process with PID 1234.

```
C:\Program Files\Palo Alto Networks\Traps> cytool policy query 1234
Enter supervisor password:
Generic
Enable 0x00000001
SuspendOnce 0x00000001
AdvancedHooks 0x00000001
[...]
```

**Compare Policies**

At regular intervals, Traps requests an updated security policy from the ESM Server and stores it in the system registry. When a user starts a process, Traps determines whether or not to protect the process based on the settings in the security policy.

In troubleshooting scenarios where Traps does not behave as expected, use the `cytool policy compare` command to view differences in policies that are applied to processes running on the endpoint. Using the command, you can compare a policy for a process to the default security policy or compare a policy for a process to a policy for another process. In both cases, you can specify either the name of the process or the process ID (PID). Specifying the process name simulates the application of the policy to the process. Specifying the PID queries the effective policy for the running process. Cytool displays the policy settings side-by-side and indicates any differences between policies in red.

To compare policies, you must enter the supervisor password when prompted.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).
**STEP 2 | Compare the details of two policies:**

- To compare the policy to the default policy, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool policy compare <process> default
```

where `<process>` is either the process name or process ID (PID).

The following example displays output for comparing a policy that applies to notepad to the default policy. Differences between the two policies are shown in red.

```
C:\Program Files\Palo Alto Networks\Traps> cytool policy compare notepad default
Enter supervisor password:
Generic
Enable 0x00000001 0x00000001
SuspendOnce 0x00000001 0x00000001
AdvancedHooks 0x00000001 0x00000001
[...]
DllSec
Enable 0x00000001 0x00000000
Optimize 0x00000001 0x000000011
[...]
```

- To compare the policies for two processes, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool policy compare <process1> <process2>
```

where `<process1>` and `<process2>` are either the process name or process ID (PID). For example, to compare the policy applied to iexplorer to the policy applied to chrome, enter `cytool policy compare iexplorer chrome`. You can also compare the policies for two PIDs or compare the policy of a process to a policy of a PID.

The following example displays output for comparing the policies applied to two PIDs, 1592 and 1000. Differences between the two policies are shown in red.

```
C:\Program Files\Palo Alto Networks\Traps> cytool policy compare 1592 1000
Enter supervisor password:
Generic
Enable 0x00000001 0x00000001
SuspendOnce 0x00000001 0x00000001
AdvancedHooks 0x00000001 0x00000001
[...]
DllSec
Enable 0x00000001 0x00000000
Optimize 0x00000001 0x000000011
[...]
```

Manage Logging of Traps Components Using Cytool

Using cytool, you can start, stop, or flush the logging of Traps drivers and services (cyverak, cyvrmtns, cyvrsfd, cyvrflpc, cyvrreport, cyserver, signer, cypriotu, cytray, cyverau, cymnjet, cyvrtrap, cyvera, ntnativeapi, winutils, tda, tdawork, analyzer, tlaservice, tlaworker, and tlaore). This enables you to troubleshoot one or more components and log errors, warnings, or information to a log file which you can
then view using the Windows Event Viewer. You can also specify the maximum file size of the log, in MB. Cytool outputs the ETL trace logs to the C:\Program Files\Palo Alto Networks\Traps\ folder.

**STEP 1** | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2** | To start logging a Traps component, use the following command:

```shell
C:\Program Files\Palo Alto Networks\Traps> cytool log start <components> [None | Critical | Error | Warning | Information | Verbose [log_size]] <max_log_size>
```

where `<components>` is either an * to start logging on all Traps services, or one or more Traps services encased in quotes and separated by spaces, for example "cyverak cyvrfsfd".

The following example displays output for using cytool to log Errors on the cyverak and cyvrmtgn files to a log file with a maximum file size of 20 MB.

```shell
C:\Program Files\Palo Alto Networks\Traps> cytool log start "cyverak cyvrmtgn" Error 20
Log session started.
```

**STEP 3** | Stop or flush the active log sessions:

- To stop logging a Traps component, use the following command:

```shell
C:\Program Files\Palo Alto Networks\Traps> cytool log stop
Log session stopped.
```

- To flush active log sessions to disk, use the following command:

```shell
C:\Program Files\Palo Alto Networks\Traps> cytool log flush
Log session flushed to directory C:\ProgramData\Cyvera\Logs.
```

**Restore a Quarantined File Using Cytool**

If a quarantined file turns out not to be malware, you can restore it using the ESM Console or by using Cytool from the endpoint.

Use the `cytool quarantine list` command to view details about all quarantined files on the endpoint. Or, to restore a file to its original location use the `cytool quarantine restore <guid>` command. To restore a file to a new location, use the `cytool quarantine restore <guid> <filepath>` command.

To view and restore quarantined details, you must enter the supervisor (uninstall) password when prompted.

> Using Cytool, you can restore a file to any non-network writable file system including NTFS, ExFAT, FAT32, FAT16, ReFS.

**STEP 1** | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2** | To view all files that Traps has quarantined on the endpoint, use the following command:
The following example displays output for using cytool to query for all quarantined files.

```
c:\Program Files\Palo Alto Networks\Traps> cytool quarantine list
Enter supervisor password:
Guid State Date/Time Path
c92e84c0-1770-40d5-b5b8-544d02381ea6 Quarantined Thursday, August 18, 2016, 14:40:21 PM C:\Malware\malware1.exe
```

**STEP 3 |** To restore a quarantined file, use the following command:

```
c:\Program Files\Palo Alto Networks\Traps> cytool quarantine restore <guid> <filepath>
```

where `<guid>` is the unique identifier of the file. If you want to restore the executable file to its original location leave the `<filepath>` blank. Otherwise, enter the location—including the filename—to which you want to restore the executable file.

The following example displays output for using cytool to restore the malware1.exe file to an alternate location.

```
c:\Program Files\Palo Alto Networks\Traps> cytool quarantine restore c92e84c0-1770-40d5-b5b8-544d02381ea6 C:\myfolder\not-malware.exe
Enter supervisor password:
Restored prevention c92e84c0-1770-40d5-b5b8-544d02381ea6 to C:\myfolder\not-malware.exe
```

**View Statistics for a Protected Process Using Cytool**

At any time you can query Traps for injection statistics on a specific protected process that is running on the endpoint using Cytool. Use the `cytool stat <pid>` command to view the injection statistics for the process.

**STEP 1 |** Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2 |** Identify the process identifier (PID) of the running process for which you want statistics. To determine which processes are being actively protected, see the Protection tab on the Traps console.
STEP 3 | To view statistics for a specific process, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool stat <pid>
```

where `<pid>` is the specific process id.

The following example displays output for using cytool to display statistics about the Chrome process with PID 4080.

```
c:\Program Files\Palo Alto Networks\Traps> cytool stat 4080
DllSec Invocations: 0
DllSec Time: 00:00:00.0
G01 Invocations: 0
G01 Time: 00:00:00.0
G01 Thunk 00 Resolution: 0
G01 Thunk 01 Resolution: 0
G01 Thunk 02 Resolution: 0
G01 Thunk 03 Resolution: 0
G01 Thunk 04 Resolution: 0
G01 Thunk 05 Resolution: 0
G01 Thunk 06 Resolution: 0
G01 Thunk 07 Resolution: 0
G01 Thunk 08 Resolution: 0
G01 Thunk 09 Resolution: 0
G01 Thunk 10 Resolution: 0
G01 Thunk 11 Resolution: 0
G01 Thunk 12 Resolution: 0
G01 Thunk 13 Resolution: 0
G01 Thunk 14 Resolution: 0
G01 Thunk 15 Resolution: 0
G01 Stack Walk Resolution: 0
J01 Minimum Stack Depth: 166
J01 Checks: 25
J01 Stack Walk Checks: 0
```

View Details About the Traps Local Analysis Module Using Cytool

Using Cytool, you can determine the current version of the Traps local analysis module.

STEP 1 | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

STEP 2 | To view the local analysis version and associated release date, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps> cytool tla query
Build: 225
Timestamp: Monday, July 18, 2016, 6:55:34 AM
```

View Hash Details About a File Using Cytool

Using Cytool, you can identify hash information about files inside of DLLs, drivers, and other portable executable (PE) files. For each file, Cytool displays the path, file size in bytes, and file hash using SHA256 encoding. If the file is a PE, Cytool also displays information about the target PE inside the file including file size, architecture type (i386 or x64), platform (for example, Win32 GUI, Win32 Console, or NT native), and
hash value. After you identify the hash associated with the target file, you can manage Hash Control from the ESM Console or you can add the hash to an SFX whitelist in the database.

Use the `cytool image "<filepath>\<filename>"` to identify hash information about a file.

**STEP 1** | Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**STEP 2** | To view hash details about a file, use the `cytool image "<filepath>\<filename>"` command. For example, the following output displays information about iexplorer.exe.

```
C:\Program Files\Palo Alto Networks\Traps> cytool image "C:\Program Files\Internet Explorer\iexplore.exe"
Image Information
Location: C:\Program Files\Internet Explorer\iexplore.exe
Size: 795.20 KB (814280 bytes)
File SHA256:
  1130c581e0e88111ec02d09ab4fc1f6d532f762c9339c7d54abaf8f43c796fe5
Architecture: x86-64
Subsystem: Windows GUI
PE Size: 780.00 KB (798720 bytes)
PE SHA256: 79dc738ce785beefcc315d004e15f2748ffd967eede830c4f9f0a59a5f6902203
```
Troubleshoot Traps Issues

This topic addresses the following issues related to Traps:

- Why can't I install Traps?
- Why can't I upgrade or uninstall Traps?
- Why can't Traps connect to the ESM Server?
- How do I fix a Traps server certificate error?

Why can't I install Traps?

**Symptom**
Traps Setup reports the following error: Service "Traps" (CyveraService) failed to start. Verify that you have sufficient privileges.

![Traps Setup Error](image)

**Possible Causes**
- You do not have administrative privileges to start services on the endpoint.

**Solution**
After each step in the following procedure, verify if you can install Traps. If Traps still reports an error, proceed to each subsequent step until the issue is resolved.

**STEP 1 |** Verify that you have administrative rights on the endpoint:

- Windows 7: Click **Start > Control Panel > User Accounts > Manage User Accounts**. On the users tab, verify that your username is in the Administrators group.
- Windows 8: Click **Start > Control Panel > User Accounts > Change User Accounts**. Verify that your account appears as an Administrator.

Log in to the endpoint as a valid administrator.

**STEP 2 |** The service log file contains information, warnings, and errors related to the Traps service. To further troubleshoot an issue related to the Traps service, open the C:\ProgramData\Cyvera\Logs\Service.log file in a text editor and review any errors in the log file that occurred at the time of the event.

*By default, the ProgramData folder may be hidden. To view the folder in Windows Explorer, select Organize > Folder and Search Options > View > Show hidden files and folders.*

**STEP 3 |** If the problems persists, contact Palo Alto Networks support.

Why can't I upgrade or uninstall Traps?

**Symptom**
Traps Setup reports the following error: Service “Traps” (CyveraService) failed to start. Verify that you have sufficient privileges.

Possible Causes
In earlier versions of Traps, the service protection feature prevents you from modifying or tampering with Traps system files.

Solution

**STEP 1** | Create an action rule to disable service protection (see Manage Service Protection).

**STEP 2** | Verify that you can install or uninstall Traps.

**STEP 3** | Delete the action rule (see Save Rules).

**STEP 4** | Try to upgrade Traps. To further troubleshoot an issue related to the Traps service, view the logs to see if Traps reports a specific error:
- From the Traps Console, select **Open Log File**.
- From the Traps Console, select **Send Support File** to send the logs to the ESM Server.
- Create an action rule to retrieve the logs from the endpoint (see Manage Data Collected by Traps).

**STEP 5** | If the problems persists, contact Palo Alto Networks support.

Why can't Traps connect to the ESM Server?

**Symptom**
Traps cannot communicate with the ESM Server to retrieve the latest security policy and reports a status of **No connection to server!**.

**Possible Causes**
- The server or endpoint specifications do not meet the installation and criteria prerequisites.
- The Traps service is down on the endpoint.
- The Endpoint Security Manager core service is down on the ESM Server.
- The endpoint is not connected to the network.
- Inbound traffic is not allowed on the port for the ESM Server (default is 2125).
- The Windows Firewall is enabled on the ESM Server and prevents the server from communicating with the client.
- The certificate on the endpoint does not match the certificate on the ESM Server (see How do I fix a Traps server certificate error?)

**Solution**
After each step in the following procedure, verify if Traps can connect to the ESM Server by selecting **Check-in now**. If Traps still can't connect to the server proceed to each subsequent step until the issue is resolved.

**STEP 1** | Verify that the server and endpoint both meet the prerequisites.
See Prerequisites.

STEP 2 | Verify that the Traps service is running on the endpoint.

1. Open the Services Manager:
   - Windows XP: From the Start Menu, select Control Panel > Administrative Tools > Services.
2. Locate the Traps service (called CyveraService in older versions of Traps) and verify that the service status is Started.
3. If the service status is Stopped, double-click the service, then select Start. Click Close.

STEP 3 | Verify that the Endpoint Security Manager core service is running on the ESM Server.

1. Open the Services Manager:
2. Locate the Endpoint Security Manager core service (called CyveraServer in older versions of the Endpoint Security Manager) and verify that the service status is Started (Windows Server 2008) or Running (Windows Server 2012).
3. If the service status is Stopped or Paused, double-click the service, then select Start. Click Close.

STEP 4 | Verify that you can reach the ESM Server from the endpoint.

From the endpoint, open a command prompt and ping the IP address or hostname of the ESM Server. If the ESM Server is unreachable, examine the network connectivity settings between the devices.

STEP 5 | Verify that you can reach the endpoint from the ESM Server.

From the ESM Server, open a command prompt and ping the IP address or hostname of the endpoint. If the endpoint is unreachable, examine the network connectivity settings between the devices.

STEP 6 | Verify that the port for the ESM Server is open on the Windows Firewall (default is 2125).

1. To check port access from the endpoint:
   1. Open a command prompt as an administrator.
   2. Enter the following command to telnet to port 2125 on the ESM Server:

   ```
   C:\> telnet <esmServerName> 2125
   ```

   where `<esmServerName>` is the hostname or IP address of the ESM Server.
2. If you are unable to telnet to port 2125, create an inbound rule to open that port:
   1. Open the Windows Firewall advanced settings:
   2. Select Inbound Rules.
   3. Create a new rule to allow Traps to communicate with the Endpoint Security Manager on port 2125 by selecting the New Rule wizard and following the guided instructions.
   3. Verify that you can now telnet to port 2125 on the ESM Server from the endpoint.
STEP 7 | Temporarily disable Windows Firewall.

1. Open the Change Action Center settings:
2. Deselect the Network firewall option.
3. Click OK.

STEP 8 | Verify that connectivity is restored between Traps and the ESM Server.

From the Traps Console, click Check-in now. If the connectivity is established, the connection status appears as Successful.

STEP 9 | View the logs to see if Traps reports a specific error:

- From the Traps Console, select Open Log File.
- From the Traps Console, select Send Support File to send the logs to the ESM Server
- Create an action rule to retrieve the logs from the endpoint (see Manage Data Collected by Traps).

STEP 10| If the problem persists, contact Palo Alto Networks Support.

How do I fix a Traps server certificate error?

**Symptom**
The following error appears in the services.log on the endpoint:

“An error occurred while making the HTTP request to https://<hostname>:2125/CyveraServer/. This could be due to the fact that the server certificate is not configured properly with HTTP.SYS in the HTTPS case. This could also be caused by a mismatch of the security binding between the client and the server.”

**Possible Causes**

When installing the ESM Server software, the following certificate configuration settings are available: No Certificate (No SSL) and External Certificate (SSL). To install Traps, you must select SSL if you selected External Certificate during the ESM Server software installation or No SSL if you selected No Certificate. The mismatch in settings causes the error reported to the service.log.

**Solution**

**STEP 1 | Reinstall the Traps software.**

Verify the SSL settings for the ESM Server and then reinstall Traps on the endpoint, taking care to select the appropriate SSL setting during installation (see Install Traps on Windows Endpoints).

**STEP 2 | Verify that the error doesn't appear in the log.**

From the Traps Console, select Open Log File, or open the services.log on the endpoint and review any recent errors. If the server certificate error persists, contact Palo Alto Networks support.
Troubleshoot ESM Console Issues

This topic addresses the following issues related to the Endpoint Security Manager (ESM) Console:

- Why can’t I log in to the ESM Console?
- Why do I get a server error when launching the ESM Console?
- Why do all endpoints appear as disconnected in the ESM Console?

Why can’t I log in to the ESM Console?

**Symptom**

The Endpoint Security Manager (ESM) Console displays an error message that the username or password is invalid.

**Possible Causes**

- The username or password was not entered correctly.
- The user specified during the initial installation does not have DB Owner privileges.
- The user was not added as an administrator.
- The user who installed the server was not a local administrator on the server.

**Solution**

**STEP 1** | Verify that you entered the correct username and password.

**STEP 2** | Verify that the user has DB Owner privileges (see Configure the MS-SQL Server Database).

**STEP 3** | Log in as an administrator and verify that the authentication mode is correct and that the user account appears on the User Management page. To add an administrative user, see Configure the Authentication Mode. Alternatively, you can add the administrator using the Database Configuration Tool (see Configure Administrative Access to the ESM Console Using the DB Configuration Tool).

**STEP 4** | If you cannot log in as an administrator, reinstall the Endpoint Security Manager as a local administrator.

**STEP 5** | Restart IIS: Click Start > Run, type IISReset, and then click OK.
STEP 6 | Verify that you can log in to the ESM Console using the account. If the problems persists, contact Palo Alto Networks support.

Why do I get a server error when launching the ESM Console?

Symptom
When opening the ESM Console, you receive an error in the browser indicating a Server Error in the '/CyveraManagement' or '/EndpointSecurityManager' Application.

Possible Causes
The server does not meet the prerequisite for .NET Framework 4.0 patched with the KB2468871 update.

Solution
Install .NET Framework 4.0 and the KB2468871 patch.

Why do all endpoints appear as disconnected in the ESM Console?

Symptom
The Health page of the ESM Console reports that all endpoints are disconnected even when the endpoint can reach the ESM Server.

Possible Causes
- The ESM Server does not meet the prerequisites.
- The Endpoint Security Manager Core service stops and must be restarted. This occurs if you wait more than one hour to install the license key after initially installing the ESM Console software.
- Inbound traffic is not allowed on the port associated with the ESM Server (default is 2125).

Solution
After each step in the following procedure, verify if Traps can connect to the ESM Server by selecting Check-in now. If Traps still can’t connect to the server proceed to each subsequent step until the issue is resolved.

STEP 1 | Verify that the server meets the prerequisites.
See ESM Server Software Requirements.

STEP 2 | Verify that the Traps service is running on the endpoint.
1. Open the Services Manager:
   - Windows XP: From the Start Menu, select Control Panel > Administrative Tools > Services.
2. Locate the Traps service (called CyveraService in older versions of Traps) and verify that the service status is Started.
3. If the service status is Stopped, double-click the service, then select Start. Click Close.

**STEP 3 | Verify that the Endpoint Security Manager core service is running on the ESM Server.**

1. Open the Services Manager:
2. Locate the Endpoint Security Manager core service (called CyveraServer in older versions of the Endpoint Security Manager) and verify that the service status is Started (Windows Server 2008) or Running (Windows Server 2012).
3. If the service status is Stopped or Paused, double-click the service, then select Start. Click Close.

**STEP 4 | Verify that the port for the ESM Server is open on the Windows Firewall (default is 2125).**

1. To check port access from the endpoint:
   1. Open a command prompt as an administrator.
   2. Enter the following command to telnet to port 2125 on the ESM Server:
      ```
      C:\> telnet <esmServerName> 2125
      ```
      where <esmServerName> is the hostname or IP address of the ESM Server.
   2. If you are unable to telnet to port 2125, create an inbound rule to open that port:
      1. Open the Windows Firewall advanced settings:
      2. Select Inbound Rules.
      3. Create a new rule to allow Traps to communicate with the Endpoint Security Manager on port 2125 by selecting the New Rule wizard and following the guided instructions.
      3. Verify that you can now telnet to port 2125 on the ESM Server from the endpoint.

**STEP 5 | Temporarily disable Windows Firewall.**

1. Open the Change Action Center settings:
2. Deselect the Network firewall option.
3. Click OK.

**STEP 6 | Verify that connectivity is restored between Traps and the ESM Server.**
From the Traps Console, click **Check-in now**. If the connectivity is established, the connection status appears as **Successful**. If the problems persist, contact Palo Alto Networks support.