## Contents

Sentry 9.13.0 Guide for Cloud .............................................................. 1

## Contents .............................................................. 2

Document history ............................................................................. 5

## About Sentry ............................................................................. 6

- Sentry overview ........................................................................ 6
- Benefits of Sentry ..................................................................... 10
- Standalone Sentry deployment scenarios ................................. 11
- Cloud, Standalone Sentry, and device interaction ...................... 14
- Persistent device list .................................................................. 16

## Standalone Sentry new features .................................................. 17

- Standalone Sentry features common to UEM platforms ............... 17
- Standalone Sentry features for Core ........................................ 18
- Standalone Sentry features for Cloud ....................................... 18

## Standalone Sentry configuration overview .................................. 19

- Configuration overview .......................................................... 19
- Accessing the Standalone Sentry System Manager ...................... 20

## Standalone Sentry for ActiveSync Email .................................... 22

- About Standalone Sentry for ActiveSync email ......................... 22
- Before you configure Standalone Sentry for ActiveSync .......... 22
- Configuring Standalone Sentry for ActiveSync ......................... 23
- 451 redirect processing .......................................................... 31
- Standalone Sentry Email+ Notification Service for Cloud ........... 31
- OAuth for Sentry on Cloud ..................................................... 39

## Standalone Sentry for AppTunnel ................................................ 49

- About Standalone Sentry for AppTunnel ................................. 49
- Before you configure Standalone Sentry for AppTunnel .......... 49
- Configuring Standalone Sentry for AppTunnel ......................... 50
- Configuring apps .................................................................... 59

## Device and server authentication .................................................. 60

- Overview .................................................................................. 60
- Configuring device and server authentication ............................ 61
- Cross-realm Kerberos support .................................................. 66
- Configuring Kerberos authentication for DFS ......................... 66

## Working with connections through Standalone Sentry .................. 68

- Standalone Sentry connections on Cloud ................................. 68
- Connections from managed devices ........................................ 68
- Unmanaged connections .......................................................... 70

## Standalone Sentry Settings ......................................................... 72

- Overview of Standalone Sentry settings ................................... 72
- Interfaces ................................................................................. 73
- Routes ...................................................................................... 76
- DNS and Hostname ............................................................... 78
- Static Hosts ............................................................................. 79
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and Time (NTP)</td>
<td>81</td>
</tr>
<tr>
<td>CLI</td>
<td>82</td>
</tr>
<tr>
<td>Splunk</td>
<td>82</td>
</tr>
<tr>
<td>Syslog</td>
<td>84</td>
</tr>
<tr>
<td>SNMP</td>
<td>87</td>
</tr>
<tr>
<td>Email Settings</td>
<td>92</td>
</tr>
<tr>
<td>Login</td>
<td>94</td>
</tr>
<tr>
<td>Timeout</td>
<td>95</td>
</tr>
<tr>
<td>Services</td>
<td>96</td>
</tr>
<tr>
<td>Sentry</td>
<td>97</td>
</tr>
<tr>
<td>Incoming SSL configuration</td>
<td>98</td>
</tr>
<tr>
<td>Outgoing SSL configuration</td>
<td>98</td>
</tr>
<tr>
<td>UEM SSL Configuration</td>
<td>98</td>
</tr>
<tr>
<td>Access SSL Configuration</td>
<td>101</td>
</tr>
<tr>
<td>Outbound HTTP Proxy</td>
<td>104</td>
</tr>
<tr>
<td>Log representation and format</td>
<td>105</td>
</tr>
<tr>
<td><strong>Standalone Sentry Security Settings</strong></td>
<td>113</td>
</tr>
<tr>
<td>Overview of Standalone Sentry security settings</td>
<td>113</td>
</tr>
<tr>
<td>Local Users</td>
<td>113</td>
</tr>
<tr>
<td>Password policy</td>
<td>115</td>
</tr>
<tr>
<td>Certificate Management</td>
<td>116</td>
</tr>
<tr>
<td>Access Control Lists</td>
<td>119</td>
</tr>
<tr>
<td>Networks and Hosts</td>
<td>122</td>
</tr>
<tr>
<td>Network Services</td>
<td>123</td>
</tr>
<tr>
<td>Access Control Lists: ACLs</td>
<td>125</td>
</tr>
<tr>
<td><strong>Standalone Sentry Maintenance Settings</strong></td>
<td>126</td>
</tr>
<tr>
<td>Overview of Sentry maintenance features</td>
<td>126</td>
</tr>
<tr>
<td>Updating Standalone Sentry software</td>
<td>126</td>
</tr>
<tr>
<td>Exporting the configuration</td>
<td>128</td>
</tr>
<tr>
<td>Importing a configuration</td>
<td>129</td>
</tr>
<tr>
<td>Clearing the configuration</td>
<td>129</td>
</tr>
<tr>
<td>Rebooting</td>
<td>130</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>131</td>
</tr>
<tr>
<td>Overview of the Standalone Sentry Troubleshooting tab</td>
<td>131</td>
</tr>
<tr>
<td>Logs</td>
<td>131</td>
</tr>
<tr>
<td>Network Monitor</td>
<td>136</td>
</tr>
<tr>
<td>Service Diagnosis</td>
<td>138</td>
</tr>
<tr>
<td>Sentry Statistics</td>
<td>139</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>142</td>
</tr>
<tr>
<td>Overview of the Standalone Sentry Monitoring tab</td>
<td>142</td>
</tr>
<tr>
<td>Alert Viewer</td>
<td>142</td>
</tr>
<tr>
<td>Alert Configuration</td>
<td>143</td>
</tr>
<tr>
<td><strong>Command Line Interface</strong></td>
<td>146</td>
</tr>
<tr>
<td>Purging the cache</td>
<td>147</td>
</tr>
<tr>
<td>Logging</td>
<td>148</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring garbage collection (GC)</td>
<td>150</td>
</tr>
<tr>
<td>Monitoring Sentry</td>
<td>151</td>
</tr>
<tr>
<td>Configuring a syslog server</td>
<td>152</td>
</tr>
<tr>
<td>Reporting</td>
<td>154</td>
</tr>
<tr>
<td>Clearing the redirect URL</td>
<td>166</td>
</tr>
<tr>
<td>Configuring access to UEM</td>
<td>167</td>
</tr>
<tr>
<td>Enabling and disabling iptables</td>
<td>167</td>
</tr>
<tr>
<td>curl</td>
<td>169</td>
</tr>
<tr>
<td>Regenerating the Standalone Sentry self-signed certificate</td>
<td>171</td>
</tr>
<tr>
<td>Checking Kerberos Key Distribution Center (KDC) connectivity</td>
<td>172</td>
</tr>
<tr>
<td>Verifying Kerberos configuration</td>
<td>173</td>
</tr>
<tr>
<td>Initializing Kerberos</td>
<td>173</td>
</tr>
<tr>
<td>Stopping and restarting Standalone Sentry services</td>
<td>174</td>
</tr>
<tr>
<td>Configuring kernel parameters</td>
<td>175</td>
</tr>
<tr>
<td>Using the Splunk forwarder service</td>
<td>176</td>
</tr>
<tr>
<td>Changing TLS protocols</td>
<td>176</td>
</tr>
<tr>
<td>Checking TLS compliance</td>
<td>177</td>
</tr>
<tr>
<td>Enabling and disabling SSL HSTS</td>
<td>178</td>
</tr>
<tr>
<td>Enabling and disabling web service HSTS</td>
<td>179</td>
</tr>
<tr>
<td>Upgrading using CLI</td>
<td>180</td>
</tr>
<tr>
<td>Configuring a proxy server for upgrades</td>
<td>182</td>
</tr>
<tr>
<td>Upgrading multiple Sentry</td>
<td>182</td>
</tr>
<tr>
<td>Viewing auto-upgrade details</td>
<td>183</td>
</tr>
<tr>
<td>Disabling auto-upgrade</td>
<td>184</td>
</tr>
</tbody>
</table>
## Document history

### Table 1. Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 11, 2021</td>
<td>Added the support for IBM Lotus Notes Traveler 11.0.1. For more information, see &quot;Standalone Sentry new features&quot; on page 17.</td>
</tr>
</tbody>
</table>


About Sentry

The following provide information about Sentry:

- Sentry overview ................................................................. 6
- Benefits of Sentry ................................................................ 10
- Standalone Sentry deployment scenarios .............................. 11
- Cloud, Standalone Sentry, and device interaction .................. 14
- Persistent device list ............................................................... 16

Sentry overview

Sentry is a part of Ivanti deployment that serves as an intelligent gatekeeper to your company’s ActiveSync server, such as a Microsoft Exchange Server, or with a backend resource such as a Sharepoint server, or it can be configured as a Kerberos Key Distribution Center Proxy (KKDCP) server. Sentry gets configuration and device information from a unified endpoint management (UEM) platform - Core or Cloud.

Access to enterprise content in business cloud services such as SalesForce, Box, G Suite, Dropbox, and Office 365 can be secured using Access. Access is a cloud service. A Access deployment requires a unified endpoint management (UEM) platform, Standalone Sentry, and Tunnel. For information about Access and how to set up the service, see the Access Guide.

The following provide additional information about Sentry:

- "Sentry flavors" below
  - "Sentry and UEM platform support" on the next page
  - "ActiveSync with Standalone Sentry" on page 8
  - "AppTunnel with Standalone Sentry" on page 9
  - "Network traffic support with AppTunnel" on page 9

Sentry flavors

Sentry is available in two flavors: Standalone Sentry or Integrated Sentry.
Standalone Sentry is a separate appliance that acts as a gateway between devices and your ActiveSync-enabled email servers or backend resource. Standalone Sentry can be configured for ActiveSync or AppTunnel, or as Kerberos Key Distribution Center Proxy (KKDCP) server. Standalone Sentry can be installed on premise on a Appliance or a virtual appliance. Or, Standalone Sentry can be installed in the cloud on AWS and Microsoft Azure.

Integrated Sentry is a Windows service that interacts with the Microsoft Exchange Server.

Sentry gets input from the unified endpoint management (UEM) platform, Core or Cloud, to do the following:

- Integrated Sentry or the Standalone Sentry configured for ActiveSync protects the ActiveSync server from wrongful access from devices.
- Standalone Sentry configured for AppTunnel provides authenticated apps secure access to the backend resource.

**Sentry and UEM platform support**

UEM support varies depending on the type of Sentry. The following tables provides the UEM supported by Sentry.

<table>
<thead>
<tr>
<th>Sentry</th>
<th>UEM platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Sentry</td>
<td>Core</td>
</tr>
<tr>
<td>Standalone Sentry (on-premise, AWS, and Microsoft Azure)</td>
<td>Core, Cloud</td>
</tr>
</tbody>
</table>

**Cloud license requirement**

Some Standalone Sentry features are available based on the license level for Cloud. The following table describes the license required for these features:
ActiveSync with Standalone Sentry

Standalone Sentry enabled for ActiveSync serves as an intelligent gatekeeper to the ActiveSync server. It uses the ActiveSync protocol to communicate with the ActiveSync server and with ActiveSync devices. For information about these interactions, see .

Exchange ActiveSync, also known as ActiveSync, is the protocol that the ActiveSync server uses to communicate over HTTP or HTTPS with devices. The ActiveSync server uses the ActiveSync protocol to do the following:

- synchronize email, contacts, calendar, tasks and notes with a mobile device
- provide for server-device interactions relating to mobile device management and policy controls

In a deployment, these devices are called ActiveSync devices. Standalone Sentry and the UEM platform work together to protect the ActiveSync server from wrongful access by these devices.

Communication between Standalone Sentry and ActiveSync servers is encrypted using HTTPS. Administrators can enable server TLS and configure outbound SSL. For Office 365 and GMail, Ivanti recommends that the communication should be configured to use HTTPS, so that confidential information such as user name, password, and email content are never communicated in clear text.

<table>
<thead>
<tr>
<th>License requirement</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>Advanced traffic control</td>
</tr>
<tr>
<td></td>
<td>Outgoing ciphers</td>
</tr>
<tr>
<td></td>
<td>CIFS service for Docs@Work</td>
</tr>
<tr>
<td></td>
<td>Sharepoint service for Docs@Work</td>
</tr>
<tr>
<td></td>
<td>Help@Work service</td>
</tr>
<tr>
<td></td>
<td>Web@Work service</td>
</tr>
<tr>
<td></td>
<td>Custom HTTP service</td>
</tr>
<tr>
<td></td>
<td>Custom TCP service</td>
</tr>
<tr>
<td>Platinum</td>
<td>Tunnel service</td>
</tr>
<tr>
<td></td>
<td>AppTunnel</td>
</tr>
</tbody>
</table>

TABLE 2. CLOUD LICENSE REQUIREMENT
**AppTunnel with Standalone Sentry**

Standalone Sentry enabled for AppTunnel provides per-app secure tunneling and access control to protect app data as it moves between the device and corporate backend resources (data-in-motion). App-by-app session security protects the connection between each app container and the corporate network. AppTunnel is particularly useful when an organization does not want to open up VPN access to all apps on the device. AppTunnel is part of an AppConnect app or a Tunnel deployment. However, AppTunnel is not a requirement for an AppConnect app deployment.

Standalone Sentry and the UEM platform work together to provide secure access to the backend resource. For example:

- UEM provides Standalone Sentry with the backend resource configuration for the app.
- When an app attempts to connect to a backend resource, Standalone Sentry creates an app tunnel which is a unique combination of user, device, and app. Standalone Sentry provides information about the app tunnel to the UEM.
- UEM informs Standalone Sentry when an app should not be allowed to access the backend resource. For example, Standalone Sentry blocks access to the backend resource if there are security policy violations or the AppTunnel is manually blocked.

**Network traffic support with AppTunnel**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP, HTTPS tunneling</td>
<td>• Android and iOS AppConnect apps</td>
</tr>
<tr>
<td>TCP tunneling</td>
<td>• Android AppConnect apps</td>
</tr>
<tr>
<td></td>
<td>• iOS and macOS managed apps with Tunnel configured for app proxy VPN.</td>
</tr>
<tr>
<td></td>
<td>• Web@Work with Chromium stack enabled.</td>
</tr>
<tr>
<td>TCP tunnels</td>
<td>TCP tunnels support HTTP and HTTPS traffic also.</td>
</tr>
<tr>
<td>IP tunneling</td>
<td>• Windows 10, iOS, and Android managed apps with Tunnel.</td>
</tr>
<tr>
<td></td>
<td>IP tunnels also support HTTP, HTTPS, TCP, and UDP traffic.</td>
</tr>
</tbody>
</table>
Benefits of Sentry

Benefits of using Sentry in your deployment include the following:

- "Device and user authentication support with Standalone Sentry" below
- "Enforcement of security policies with Sentry" below
- "Visibility into which devices are accessing the backend resource with Sentry" below
- "Ability to take action on ActiveSync device with Sentry" on the next page

Device and user authentication support with Standalone Sentry

Using Standalone Sentry, you can choose how the user authenticates with the ActiveSync server or the backend resource. You can choose password authentication, certificate authentication, or Kerberos Constrained Delegation.

Enforcement of security policies with Sentry

UEM applies security, privacy, lockdown, and sync policies to registered devices. These policies ensure that devices can connect only if they comply to your organization’s security requirements. Standalone Sentry gets device posture and compliance information from UEM, and allows access based on the device posture.

Visibility into which devices are accessing the backend resource with Sentry

When using Standalone Sentry for ActiveSync or AppTunnel, devices access the backend resource through Standalone Sentry. Because of this single point of access, Standalone Sentry knows which devices and users are accessing backend resources.

Standalone Sentry for ActiveSync creates a unique record for each combination of user and device accessing the ActiveSync server. Standalone Sentry then associates the ActiveSync record to a device and user in UEM. Without Sentry, a user could configure multiple devices to access the ActiveSync server, and you would have no automated way of knowing about all the devices or managing access for these devices.

Standalone Sentry for AppTunnel creates a unique AppTunnel session (connection) for each unique combination of user, app, and device. For example, Standalone Sentry creates an AppTunnel for UserA using AppA on DeviceA, and a new AppTunnel for UserA using AppB on DeviceA. Each AppTunnel provides visibility into the user, device and the backend resources being accessed.
Ability to take action on ActiveSync device with Sentry

Cloud

If there are policy violations, registered ActiveSync devices and AppTunnels can be blocked. You can take Allow, Block, and Remove actions on unregistered ActiveSync devices.

Standalone Sentry deployment scenarios

In a deployment, Standalone Sentry works with the UEM platform secures access to backend resources by preventing wrongful access from devices. The UEM can be Core on a Physical or Virtual Appliance or it can be a Cloud deployment. This section provides various deployment scenarios with Standalone Sentry.

These deployments include:

- "Deployment with Standalone Sentry in the DMZ" below
- "Deployment with multiple Standalone Sentry servers" on the next page
- "Deployment with Standalone Sentry behind a proxy" on page 13
- "Deployment with multiple ActiveSync servers or backend resources" on page 14

Deployment with Standalone Sentry in the DMZ

The following illustration shows Standalone Sentry in a configuration in which Standalone Sentry is located in the DMZ along with UEM:

**Figure 1. Standalone Sentry and UEM located in the DMZ**
Standalone Sentry can be located in the DMZ, along with UEM, but this configuration is not required. You can alternatively:

- Put Standalone Sentry in the DMZ and put UEM behind the corporate firewall.
- Put UEM in the DMZ and put Standalone Sentry behind the corporate firewall.
- Put both Standalone Sentry and UEM behind the corporate firewall.

**Deployment with multiple Standalone Sentry servers**

Use multiple Standalone Sentries in the following situations:

- Your ActiveSync server has more users than one Standalone Sentry can support.

A Standalone Sentry has an upper limit for the number of registered ActiveSync devices that it can support, depending on its configuration. If your ActiveSync server supports more devices than this limit, use multiple Standalone Sentries. Configure each Standalone Sentry to point to the same ActiveSync server (or servers if multiple ActiveSync servers back each other up). For more information about Standalone Sentry capacity, see the *Standalone Sentry On-Premise Installation Guide*.

**Figure 2. Deployment with multiple Standalone Sentries**

- You have multiple ActiveSync or backend resources, each of which supports a different organization.

Use one Standalone Sentry for each organization. Configure the Standalone Sentry to point to the server (or servers if multiple servers back each other up) for that organization.

- You have ActiveSync or backend resources in different locations.
If you have ActiveSync or backend resources in different locations, use a Standalone Sentry for each location. By co-locating the Standalone Sentry with the ActiveSync or backend resource, you minimize latency between Sentry and the server. Configure each Sentry to point to its co-located server (or servers if multiple servers back each other up).

**FIGURE 3. SENTRY IN DIFFERENT LOCATIONS**

Typically, you use load balancers when using multiple Standalone Sendrys. For information about using load balancers with Standalone Sentry, contact Professional Services.

For more information about deploying Standalone Sentry for high availability and load balancing, see the following knowledge base articles:

- [Sentry HA Networking Overview and Recommendations](#)
- [Mail Server Resource Consumption](#)

**Deployment with Standalone Sentry behind a proxy**

You can configure the Standalone Sentry to be deployed behind a proxy, for example, an Apache or an F5 server. This allows for SSL termination to occur in front of Sentry even when using certificate based authentication.

By terminating SSL in the DMZ, Standalone Sentry enables an added layer of security, as well as accommodates the DMZ firewall policies.

Leveraging this configuration requires:

- Setting up an Apache or F5 proxy to front-end the Standalone Sentry.
• Enabling this feature on Sentry via the UEM UI.
• Additional minor changes to references to hostname in some profiles.

Contact Professional Services or a certified partner to set up this deployment.

**Deployment with multiple ActiveSync servers or backend resources**

You can configure one Standalone Sentry to work with multiple ActiveSync servers or backend resources that are backing each other up. You control when Standalone Sentry switches to another ActiveSync Server or backend resource by setting parameters involving communication failures between Standalone Sentry and the active ActiveSync servers or backend resource.

**Cloud, Standalone Sentry, and device interaction**

The following describe Core, Standalone Sentry, and device interaction:

- "When an ActiveSync device accesses email" below
  - "When an app accesses the backend resource" on the next page
  - "When Cloud detects a security policy violation" on page 16
  - "When Sentry initializes" on page 16
  - "Periodic Standalone Sentry check in with Cloud" on page 16

**When an ActiveSync device accesses email**

The following illustrates the interaction between Standalone Sentry, UEM, and the device when the device *first* attempts to access the ActiveSync server.

**Figure 1. Device first attempt to access the ActiveSync server**

1. Device attempts to access the ActiveSync server.
2. Sentry queries Cloud for registered devices and unregistered tunnels that might match the device.
Sentry checks for unregistered tunnels to ensure that the device is not already allowed on a different Sentry registered to Cloud.

3. Standalone Sentry correlates the list provided by Cloud and picks the best match based on the following criteria: Active Sync ID, User ID. If a match is found, Sentry does additional checks to ensure that the device is in compliance before allowing or blocking the device access to the ActiveSync server.

4. Standalone Sentry adds the device to its list of devices.

5. If access is allowed, device continues email processing.
   If access is blocked, the device will not be able to process email through Standalone Sentry.

6. Standalone Sentry checks in with Cloud, at the next check-in interval, to update Cloud with the tunnel (activesync and app) inventory in its list.

The next time a device attempts to access the ActiveSync server, the device is already in the Standalone Sentry’s list. Standalone Sentry periodically checks in with Cloud to update the compliance status for the device. The device is either allowed or blocked access based on the compliance status.

If Standalone Sentry cannot communicate with Cloud

Allowing or blocking new device access to the ActiveSync server, if Cloud is not accessible, is configured on Cloud.

1. Based on the setting in Cloud, Standalone Sentry either allows or blocks access to the ActiveSync server.
2. When the connection is reestablished, Standalone Sentry evaluates the status of the device following the steps described in "When an ActiveSync device accesses email" on the previous page.

When an app accesses the backend resource

When using Standalone Sentry for AppTunnel, when an app first attempts to access the backend resource, the following occurs:

1. UEM tells Standalone Sentry whether to allow or block the app’s access to the backend resource based on:
   - the device’s security policy and traffic control rules
   - whether the app is an authorized app
2. Standalone Sentry creates an AppTunnel for the app to access the backend resource based on the AppTunnel status provided by the UEM.
3. The AppTunnel view on the UEM now includes the new AppTunnel.
4. The next time the app attempts to access the backend resource, the app uses the AppTunnel that was created to access the backend resource.

On the first attempt, if Standalone Sentry is temporarily unable to communicate with the UEM due to, for example, a network error, the following occurs:
1. Standalone Sentry allows the app to access the backend resource.
2. At the periodic Sentry check in with Cloud, the UEM sends Standalone Sentry the proper state of the device (allowed, blocked, or wiped).

**When Cloud detects a security policy violation**

Cloud detects a security policy violation when, for example, a device checks in. At the periodic Cloud-Sentry check in, Standalone Sentry get the updated status for the devices and blocks the device from accessing the ActiveSync server and backend resources if Cloud is configured so that Sentry blocks the device.

**When Sentry initializes**

When Standalone Sentry starts or restarts, the following occurs:

1. When a device attempts to access the ActiveSync server it is as though it is the first time. See "When an ActiveSync device accesses email" on page 14.
2. Standalone Sentry retrieves the AppTunnels equal to the Sentry device cache size (number).

**Periodic Standalone Sentry check in with Cloud**

Standalone Sentry periodically checks in with Cloud to do the following:

- Get the updated compliance status for devices.
- Get any administrator actions taken on tunnels. Example: If a tunnel is blocked, Standalone Sentry retrieves the blocked status when it periodically checks in with Cloud.
- Update Cloud with the tunnel (ActiveSync and app) inventory in its list.

These are separate check ins with Cloud and occur on different schedules.

**Persistent device list**

Standalone Sentry operates using a list of ActiveSync devices that it keeps in its memory. This list is sometimes called the device cache. The information includes each device's state, such as allowed or blocked.

**Checking if Standalone Sentry can reach UEM**

You can check whether Standalone Sentry can reach UEM by using the Standalone Sentry System Manager. See "Service Diagnosis" on page 138.
Standalone Sentry new features

For new features and enhancements provided in previous versions, see the release notes for those versions.

The following are new features and enhancements available in this release and are divided into the following categories:

- “Standalone Sentry features common to UEM platforms” below
- “Standalone Sentry features for Core” on the next page
- “Standalone Sentry features for Cloud” on the next page

Standalone Sentry features common to UEM platforms

The following new Standalone Sentry features and enhancements are available for the UEM platforms:

- **Support for IBM Lotus Notes Traveler**: IBM Lotus Notes Traveler 11.0.1 is now supported with this release.
- **Support for VMware ESXi 7.0**: VMware EXSi 7.0 is now supported for Sentry 9.13.0.
- **Support for AWS inplace upgrade**: The AWS inplace upgrade is now supported with Sentry 9.13.0.
- **Support to enable HSTS on web services that talk to web browsers**: Enabling HSTS (RFC 6797) enforces secure HTTPS connection between web services that talk to the web browsers and Standalone Sentry. By default, HSTS is disabled. For more information, see Enabling and disabling web service HSTS.
- **Validate signature for authentication requests**: When configuring a Federated Pair in Access, the checkbox labeled “Validate signature for authentication requests” should be enabled. For backward compatibility, this option is unchecked for the existing pairs. Ensure that the SP/IdP metadata is updated and enable the checkbox.
- **Support for Netapp ONTAP share v9.6P4**: Netapp ONTAP share v9.6P4 is now supported with Standalone Sentry 9.13.0.
- **Support for open-vm-tools**: The open-vm-tools rpm is now installed by default when Sentry runs on VMware platform and is not required to install the VMware tools manually. For more information, see “Installing VMware tools” in the Standalone Sentry Installation Guide.
- **Support to add Login Banner**: Login Banner can now be added to display official government disclaimers. For more information, see [Login](#).

- **Support to add idle Timeout**: You can now add idle session timeout for Sentry System Manager. For more information, see [Timeout](#).

### Standalone Sentry features for Core

There are no new Standalone Sentry features and enhancements available for Core only.

### Standalone Sentry features for Cloud

There are no new Standalone Sentry features and enhancement available for Cloud only.
Standalone Sentry configuration overview

Configuration overview

You configure the initial setup of Standalone Sentry as part of the installation process. Additional Standalone Sentry configuration for ActiveSync, AppTunnel, certificates, and preferences occurs on the UEM. These settings specify how Sentry connects to the UEM, the ActiveSync server, backend resources, and to devices. Standalone Sentry system management occurs on the Sentry System Manager.

- "Initial setup" below
- "Standalone Sentry configurations on Cloud" below
- "Standalone Sentry System Manager" on the next page

Initial setup

Initial setup is part of the Sentry installation process. You configure the Sentry administrator, network setup, including the Sentry IP address and FQDN, as part of the initial setup. For information see the MobileIro Standalone Sentry Installation Guide.

Before continuing with Sentry configuration using the UEM administrative portal, ensure that you have installed Standalone Sentry.

Standalone Sentry configurations on Cloud

For Standalone Sentry configurations on Cloud, see the following:

- "Standalone Sentry for ActiveSync Email" on page 22
- "Standalone Sentry for AppTunnel" on page 49
- "Device and server authentication" on page 60
**Standalone Sentry System Manager**

Settings in the System Manager include Standalone Sentry’s host name, network address, interfaces, and routes, the certificate for accessing the Sentry System Manager, and log management.

For more information, see:

- "Standalone Sentry Settings" on page 72
- "Standalone Sentry Security Settings" on page 113
- "Standalone Sentry Maintenance Settings" on page 126
- "Troubleshooting" on page 131
- "Monitoring" on page 142

**Accessing the Standalone Sentry System Manager**

The following provides the steps to access the Standalone System manager.

**Procedure**

1. Enter the following URL in browser:
   
   ```
   https://<fully_qualified_hostname>:8443
   ```
   
   The following screen displays.

   **NOTE:** The version number will change depending on the version of the Standalone Sentry.

   **Figure 1. Standalone Sentry Sign in**

   ![Standalone Sentry Sign in](image)

2. Enter a user ID and password for the Standalone Sentry.
You can enter the administrator ID and password specified during installation of Sentry. You can also enter credentials for any local users created on this Sentry after installation. The user ID is case sensitive.

**FIGURE 2. STANDALONE SENTRY SYSTEM MANAGER**

**TIP:** To log out of the Sentry web portal, click **Sign Out** in the upper right corner.

**Related topics**

"Standalone Sentry System Manager" on the previous page
Standalone Sentry for ActiveSync Email

About Standalone Sentry for ActiveSync email

Standalone Sentry is a part of Ivanti deployment that provides secure access to your company’s ActiveSync server, such as a Microsoft Exchange Server.

You configure Standalone Sentry for email in the UEM platform. Configuring Standalone Sentry for email is a two-step process.

1. Configure a Standalone Sentry for ActiveSync in the UEM platform.
2. Create an Exchange setting in the UEM, which points to the Standalone Sentry.
   Despite its name, you configure an Exchange app setting regardless of whether your ActiveSync server is a Microsoft Exchange Server or another type of ActiveSync server, such as a Lotus Domino server.

Before you configure Standalone Sentry for ActiveSync

1. You must have installed Standalone Sentry. See the Standalone Sentry Installation Guide.
2. If your UEM is Cloud, the Standalone Sentry must be registered to your Cloud instance.
3. You must have the required certificate setup in your UEM.
   ActiveSync uses either pass through or Identity certificate for device authentication and pass through or Kerberos for server authentication. The Identity certificate can be local or a trusted CA. If you are using an Identity certificate, you will upload the Identity certificate in the Sentry configuration you create on your UEM.

Configuring authentication using SCEP Identity (Cloud only)

For Cloud only, if you intend to use a SCEP identity certificate you must add the certificate to Cloud and create the associated App Identity Certificate configuration.

Procedure
1. Add a local or external certificate authority in Admin > Certificate Authority.
   A Connector installation is required if you are using an external certificate authority.
2. Add an App Identity Certificate Configuration. This is the SCEP identity you will use when you configure device authentication in the Standalone Sentry configuration.
3. Create an Identity Certificate setting, in **Configurations > Add > Identity Certificate**. For **Certificate Distribution**, select **Dynamically Generated** and for **Source**, select the certificate you configured in **Admin > Certificate Authority**. You will reference the Identity Certificate configuration when you create the Exchange configuration.

**Configuring Standalone Sentry for ActiveSync**

You configure a Standalone Sentry for ActiveSync by configuring the Standalone Sentry profile with an ActiveSync Service in Cloud.

**Procedure**

1. In Cloud, go to **Admin > Sentry**.
2. Click **+Add Sentry Profile** or click on an existing profile to **Edit**.
3. Depending on the device authentication you will configure, select one of the following:
   - **ActiveSync with basic auth**
   - **ActiveSync and/or App Tunnel with certificates**
   - **ActiveSync and/or App Tunnel with Kerberos**
4. Use the guidelines provided in the following sections to configure Standalone Sentry for ActiveSync.
   - "Configuring Standalone Sentry connectivity settings" below
   - "Device Authentication" on the next page
   - "Default unmanaged devices behavior" on the next page
   - "Passive health check options" on the next page
   - "Scheduling options" on page 25
   - "Default HTTP/TCP timeouts" on page 25
   - "Sentry server configuration" on page 26
   - "ActiveSync service" on page 29
5. Click **Save**.

**Configuring Standalone Sentry connectivity settings**

The following table describes the Standalone Sentry connectivity settings.
**Table 1. Standalone Sentry Connectivity Settings**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sentry Host / IP</td>
<td>Enter the host name (FQDN) or IP address of the server on which the Standalone Sentry is installed. The host name or IP address must be external so that apps that are tunneling data are able to access the Sentry.</td>
</tr>
<tr>
<td>Sentry Port</td>
<td>Enter the port where mobile devices will connect to Standalone Sentry. Enter 443.</td>
</tr>
</tbody>
</table>

**Device Authentication**

Device authentication determines how users attempting to connect to the ActiveSync server or backend resource authenticate with Standalone Sentry. AppTunnel setup requires an Identity certificate or a Kerberos setup.

See "Device and server authentication" on page 60 for information on selecting and configuring a method of device authentication.

**Default unmanaged devices behavior**

By default, Sentry blocks unregistered devices from accessing backend resources. Use this setting to change Sentry’s behavior to allow unregistered devices access to backend resources. Irrespective of this setting, you will be able to allow or block devices on a per-device basis.

**Table 2. Default unmanaged devices behavior field description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow unmanaged devices to receive email and data</td>
<td>Check to allow unregistered devices access to backend resources.</td>
</tr>
</tbody>
</table>

**Passive health check options**

These settings determine when a Sentry is marked as ‘dead’. If a server fails more than the number set in Dead Threshold within the time set in Failure Window, then it is marked as dead for the time set in Dead Time.
### Table 3. Passive Health Check Field Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dead Threshold</td>
<td>Specify the number of times that a server connection can fail before the server will be marked “dead”. The valid range is 1 through 1000.</td>
</tr>
<tr>
<td>Failure Window</td>
<td>Specify the time interval in milliseconds during which the specified number of server connection failures must occur in order for the server to be marked “dead”. The valid range is 1 through 86400000 milliseconds (24 hours).</td>
</tr>
<tr>
<td>Dead Time</td>
<td>Specify the amount of time in milliseconds that the server should be marked “dead” after the specified number of connection failures. The valid range is 1 through 172800000 milliseconds (48 hours).</td>
</tr>
</tbody>
</table>

### Scheduling Options

The options provide additional flexibility in managing multiple Sentrys. Specify Priority or Round Robin scheduling if multiple servers are specified.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The first available server in the specified list will be used, with the first server in the list having highest priority. So if the first server in the list is never unavailable, then the other servers will never be used.</td>
</tr>
<tr>
<td>Round Robin</td>
<td>Each server in the list will be used in turn.</td>
</tr>
<tr>
<td></td>
<td>By default, Round Robin is enabled.</td>
</tr>
</tbody>
</table>

### Default HTTP/TCP Timeouts

These settings provide additional flexibility to configure Standalone Sentry session timeouts. You may want to configure the session timeouts to manage server resources.

**WARNING:** Do not make changes to the settings unless specifically instructed in the documentation or by Professional Services.
**Table 5. Default HTTP/TCP timeouts field description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Socket read/write timeout</td>
<td>Specify the time in milliseconds, the Sentry should check for the socket read/write time out from either the device or the server. Enter a valid integer. The default setting is 10000, and the minimum is 1.</td>
</tr>
<tr>
<td>Server connection timeout</td>
<td>Specify the time in milliseconds after which the Sentry will time out when connecting to the server. Enter a valid integer. The default setting is 10000, and the minimum is 1.</td>
</tr>
<tr>
<td>Server response timeout</td>
<td>Specify the time in milliseconds after which the Sentry will time out when waiting for an HTTP response from the server. Enter a valid integer. The default setting is 60000, and the minimum is 1.</td>
</tr>
<tr>
<td>Device request timeout</td>
<td>Specify the time in milliseconds after which the Sentry will time out when waiting for an HTTP request from the device on a new or existing connection. Enter a valid integer. The default setting is 10000, and the minimum is 1.</td>
</tr>
</tbody>
</table>

**Sentry server configuration**

Configure the Sentry port, certificate, protocols and cipher suites.

- "HTTPS Port" below
- "Certificate/Key " on the next page
- "Protocols and cipher suites" on the next page
- "Load balancers and ciphers" on the next page
- "Supported protocols" on page 28

**HTTPS Port**

The default is 443. This is the port Sentry listens on for connections from the mobile devices.
Certificate/Key

When you first install Standalone Sentry, a self-signed certificate is also installed. Ivanti strongly recommends that you replace the default certificate with a publicly trusted certificate.

Protocols and cipher suites

Standalone Sentry uses the ciphers and protocols defined here for incoming traffic from device to Standalone Sentry and outgoing traffic from Standalone Sentry to backend resources. Ciphers and protocols for incoming traffic is set in the Incoming tab. Ciphers and protocols for outgoing traffic is set in the Outgoing tab.

You can do the following:

- View the available and selected protocols and cipher suites.
- Setup custom protocol and cipher suite configuration.
- Enable SNI. (Outgoing only)

A default set of cipher suites and protocols are selected. You can customize the selected list of ciphers and protocols to match the security and system needs for your enterprise.

The available and default set of cipher suites and protocols may be updated in a release. Some cipher suites and protocols may be added, while others may be removed. Cipher suites and protocols may be removed if the platform no longer supports these cipher suites and protocols.

If you are set up to use the default cipher suites and protocols, these will be updated to the latest defaults. If you are set up to use a custom list of selected cipher suites and protocols, the custom list is preserved. However, any cipher suites or protocols that are not supported by Standalone Sentry are ignored and noted in Monitoring in Standalone Sentry System Manager.

WARNING: Making changes to the default list of cipher suites may impact the performance and security of traffic through Standalone Sentry. Therefore, before making any changes to the selected cipher suites, Ivanti recommends that you understand both the performance and security impact of the changes.

Load balancers and ciphers

If you use a load balancer to perform HTTPS/GET checks against your Sentry and your Sentry uses strong ciphers, do the following:

- Make sure the ciphers enabled in your HTTPS/GET check match one of Sentry’s strong ciphers.
• If you cannot change the ciphers that your HTTPS/GET check uses, you can change your check to use HTTP/GET to accomplish the same monitoring.

**Supported protocols**

• TLSv1
• TLSv1.2
• TLSv1.1
• SSLv2Hello

**Note The Following:**

• SSLv2Hello is a pseudo-protocol that allows Java to initiate the handshake with an SSLv2 'hello message.' This does not cause the use of the SSLv2 protocol, which is not supported by Java. SSLv2Hello requires that TLSv1 protocol is also selected.

SSLv2Hello is required by some load balancers and SSL off loaders for proper functioning. If your environment does not need it, it is recommended to remove this from the protocol list for improved security.

**SNI**

Server Name Indication (SNI) is an extension to TLS. SNI allows multiple hostnames to be served over HTTPS from one IP address. By default, SNI is disabled on Standalone Sentry for outgoing connections.

SNI allows a load balancer to direct incoming traffic to the correct backend server based on the hostname provided by the client, in this case, Standalone Sentry. Some backend server may require that SNI is enabled in the client.

Your Active Directory Federation Services (ADFS) may require SNI for all client communications.

---

If SNI is enabled for Outgoing SSL connections, in some cases health check may fail if the backend server does not also support SNI. The workaround is to disable health check for the impacted server.

**Advanced Traffic Control and server-side explicit proxy**

These settings are not applicable for configuring an ActiveSync service on Standalone Sentry.
**ActiveSync service**

In the Sentry profile, in **Manage Services**, configure **Exchange ActiveSync** to set up an ActiveSync service.

The following table describes the settings for configuring an ActiveSync service.

**TABLE 6. FIELD DESCRIPTIONS FOR ACTIVESYNC SERVICE**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The <strong>Service Name</strong> identifies the ActiveSync service. A service name cannot contain these characters: 'space' ; * ? &lt; &gt; &quot;</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Server TLS</td>
<td>Specify whether the ActiveSync servers require SSL (i.e., port 443).</td>
</tr>
<tr>
<td></td>
<td>If you are using Google Apps via Standalone Sentry, you must check Enable Server TLS.</td>
</tr>
<tr>
<td>Enable Redirect Processing (451)</td>
<td>To disable redirect processing, clear the check box.</td>
</tr>
<tr>
<td></td>
<td>If Enable Redirect Processing (451) is disabled, the Standalone Sentry does not handle redirection, and passes the redirect URL to the device.</td>
</tr>
<tr>
<td></td>
<td>See also &quot;451 redirect processing&quot; on the next page.</td>
</tr>
<tr>
<td>Enable Active Health Check</td>
<td>The default setting is enabled. Clear the check box to disable the ActiveSync server health check.</td>
</tr>
<tr>
<td></td>
<td>If enabled, when the ActiveSync server fails for the number of times configured in the Dead Threshold setting and within the number configured in the Failure Window, then the ActiveSync server status shows Unreachable.</td>
</tr>
<tr>
<td></td>
<td>When the background health check determines that the server is live for the number configured for Live Threshold, the ActiveSync server status shows Reachable.</td>
</tr>
</tbody>
</table>

**Configuring Exchange settings for Standalone Sentry**

The Exchange setting is pushed to the device and points to the Standalone Sentry.

**Procedure**

1. In the Cloud, go to **Configurations**.
2. Click **+Add > Exchange**.
3. For Server address, enter one of the following:
   - When using Standalone Sentry, set the server address to the Standalone Sentry's address.
   - When using Standalone Sentry with Lotus Domino server 8.5.3.1 Upgrade Pack 1, set the server address to `<Standalone Sentry's fully qualified domain name>/traveler`.
   - When using Standalone Sentry with a Lotus Domino server earlier than 8.5.3.1 Upgrade Pack 1, set the server address to `<Standalone Sentry’s fully qualified domain name>/servlet/traveler`.
   - If you are using load balancers, contact Professional Services.
4. Enter the variable for the ActiveSync User.
5. Enter the variable for the ActiveSync user Email.
6. Enter the ActiveSync user Account Password.
7. If Standalone Sentry is using Identity or Group certificate for device authentication, select the **Identity Certificate** configuration to generate the identity certificate for the device.
8. After completing the form, click **Next**.
9. Select the distribution option and click **Done**.
Related topics

See “Exchange Configuration” in the Cloud Guide or help to complete the fields in the form.

451 redirect processing

If 451 redirect URL is set up on your ActiveSync server, Standalone Sentry handles the redirection when a device tries to sync. The redirect URL is not forwarded to the device.

You configure 451 redirect processing on the Standalone Sentry by enabling or disabling the Enable Redirect Processing (451) field in the ActiveSync service. Redirect processing is enabled by default.

Standalone Sentry Email+ Notification Service for Cloud

You must configure Standalone Sentry on Cloud and key-value pairs of the Email+ application to receive email notifications on the device. The configuration is required for Standalone Sentry to act as a Email+ Notification Service to deliver notifications. This feature is available only when it is used with Email+ 3.13.0.

Before you begin

- Ensure that you have Cloud 74 and Sentry 9.10.0 or later.

- Ensure that you have the JWT token of CNS production server. A token is a randomly generated string from Ivanti, representing an authorization token for the cloud server. The term JWT token is also referred as Authorization Token, Token, and notification_server_authorization across Ivanti products.

- Standalone Sentry must be configured with a publicly trusted certificate.

- Ensure that the Exchange servers are configured with the service account. The servers must have identity certificate to authenticate the service account. For more information on configuring service account on Microsoft Exchange server, see “Configuring a service account” on page 37. Also, see Microsoft documentation.

- If Exchange server version support is earlier than TLS v1.2, then the supported protocols should be configured in Incoming SSL configuration protocols on MICS.

Procedure

1. On Cloud, click Admin

2. Under Infrastructure, click Sentry > + Add Sentry Profile

3. Select Email+ Notification Service and click Next.
4. In Global Settings, enter a profile **Name** and **Notification Server Hostname** (Sentry hostname). The port is set at 443.

5. Verify the **Sentry Server Configuration** and click **Next**.
NOTE: These fields are at default values. Ensure that the TLS certificate is a third party trusted certificate.
6. Under **Services > Manage Services**, click **Email+ Notification Service**.

7. Enter the following details:

   - **Notification Server Authorization**: The token received after registering for the Cloud Notification Service.
   
   - **Add the Service Account**: Click Add to upload the Exchange Service account certificate.
   
   - **Add the Exchange Server**: Click Add to add the desired Exchange Server. The port is set at 443.
Retain the other fields at default values.

8. On Standalone Sentry, register Sentry to Cloud using CLI.
   "registration tenantadminuser".
9. Under **Sentry > Sentry Profiles**, click **Actions** to assign the registered Sentry to the ENS profile created above.

**Sentry**

**Show Description**

- **Download installer**
- **Add Sentry Profile**

**Unconfigured Sentry Servers**

The following Sentry servers are registered but not assigned to any Sentry Profile.

<table>
<thead>
<tr>
<th>SENTRY HOSTNAME</th>
<th>SERVER SIZE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-10-84-98-121</td>
<td>small</td>
<td>Sentry Standalone 9.8.1 Build 21</td>
</tr>
</tbody>
</table>

**Sentry Profiles**

**ENS profile**

<table>
<thead>
<tr>
<th>SENTRY HOSTNAME</th>
<th>SERVER SIZE</th>
<th>VERSION</th>
<th>STATUS</th>
<th>LAST CON</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There is no information to display.
10. On Cloud, click **Apps > App Catalog > Add** to add the Email+ configuration. Select the appropriate configuration for the Email+ application and under **Apps Configurations**, enter the following details.

<table>
<thead>
<tr>
<th>Add App</th>
<th>Cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose</td>
<td></td>
</tr>
<tr>
<td>Describe</td>
<td></td>
</tr>
<tr>
<td>Delegate</td>
<td></td>
</tr>
<tr>
<td>Distribute</td>
<td></td>
</tr>
<tr>
<td>Configure</td>
<td></td>
</tr>
</tbody>
</table>

![MobileIron Email+](image)

**Email+ Settings**

- **Email Address**: Enter the email address of the device user. Type $ to see a list of variables to use for this field.
- **Email Password**: Enter the user’s password for the ActiveSync server. Type $ to see a list of variables to use for this field.
- **Exchange Host**: exchangeentry.com
- **Exchange Username**: $userEmailAddress

- **Minimum Characters for GAL Search**: 4

11. Click **Done**.

**Next steps**

You must configure the key-value pairs for Email+ notification services. For more information, see "Additional configurations using key-value pairs" in the *Email+ Guide*.

**Configuring a service account**

Service account on Microsoft Exchange impersonates other mailboxes when accessing exchange over various supported protocols. Following are the main steps for configuring service account.

- Setting up service accounts on Exchange server
- Configuring a service account on Exchange server
Setting up service accounts on Exchange server

For the purpose of Exchange Notification Proxy (ENP), Microsoft’s Exchange Web Services (EWS) protocol is used to access mailbox messages. For example service account is assigned to the following role:

ApplicationImpersonation

The EWS sends requests with the credentials of a single service account which includes an .XML key.

```xml
<soap:Header>
  <t:RequestServerVersion Version="Exchange2013" />
  <!-- The following causes the request to run as alfred@contoso.com -->
  <t:ExchangeImpersonation>
    <t:ConnectingSID>
      <t:SmtpAddress>alfred@contoso.com</t:SmtpAddress>
    </t:ConnectingSID>
  </t:ExchangeImpersonation>
</soap:Header>
```

This allows a single account to access the mailbox of other accounts.

Configuring a service account on Microsoft Exchange server

Procedure

1. In the Microsoft Exchange Management console, open a browser and type in URL. For example: https://<hostname>/ecp

2. Log in as an Admin, go to Mail > Options > Manage My Organization > Roles & Auditing > Mailboxes and create a new Role group.

3. Add the applicationImpersonation role to the group.

4. Add members to the group.

5. Click Save to finish.

For more information on configuring service account on Microsoft Exchange server, see Microsoft documentation.

A device authenticating to Core with a certificate is also known as certificate-based authentication (CBA) to Core.
OAuth for Sentry on Cloud

OAuth is supported with Standalone Sentry for Office 365. The following scenarios must be compliant for OAuth to function correctly:

- The email client must support OAuth (iOS Native Mail, iOS Email+ and Android Email+)
- UEM must push an OAuth configuration to the email client
- UEM must enable Sentry for OAuth

Configuring Sentry on Cloud for OAuth

You must configure Sentry to enable OAuth and provide the endpoints.

Before you begin

- Verify that you have Sentry 9.12.0 or later and Cloud 75 or later.

Procedure

1. Login to Cloud with admin credentials.
2. Click **Admin > Sentry > Add Sentry Profile.**

Choose Authentication

The type of authentication will determine how you can use the Sentry servers that are assigned to this profile.

1. Go to the **Add Configuration** section to add a new configuration.
2. Select **ActiveSync with Basic Auth and/or OAuth** to add your new app identity certificate configuration.
3. Under the Certificate Distribution drop-down, select "Dynamically Generated".
4. Once created, your new configuration will appear under the Configurations list like this.

3. Select **ActiveSync with Basic Auth and/or OAuth** and click **Next.**
4. Enter the **Name, Hostname,** and **Port** details and click **Next.**
5. Enter the Sentry Server Configuration details and click **Next**.
6. Click **Exchange ActiveSync** and enter the following details:

   - **Destination OAuth2 Authorization Endpoint:**
     [https://login.windows.net/common/oauth2/authorize](https://login.windows.net/common/oauth2/authorize)
   - **Destination OAuth2 Token Endpoint:** [https://login.windows.net/common/oauth2/token](https://login.windows.net/common/oauth2/token)
   - **Sentry Resource:** [https://<SentryHostname>](https://<SentryHostname>)
7. Click **Next > Save**.

**Configuring iOS native email configuration with OAuth**

You must enter the Sentry OAuth Sign In URL.
Before you begin

Verify that you have added the Sentry profile with OAuth settings.

Procedure

1. Login to Cloud with admin credentials.

2. Click **Configurations** > **Add** > **Exchange**.

3. Enter the name and description.

4. In Configuration Setup, select **Enable OAuth for exchange payload**.

5. Enter the following details:

   a. **OAuth Sign In URL**: https://<Sentry HostName>/proxyservice/oauth2/authorize

   b. **OAuth Token Request URL**: https://<Sentry HostName>/proxyservice/oauth2/token

6. Click **Next > Done**.
Configuring Android and iOS Email+ configuration with OAuth

1. Login to Cloud with admin credentials.
2. Click Apps > App Catalog > Add.
3. Select Email+ 3.8.0. (Android AppConnect) for Android configuration.
4. Enter the details and click **Next** to add the application.
Figure 1. Android Email+ Configuration
App Configurations Summary • Email+ Configuration

Configuration Setup

Name
Email+ Config

Description
N/A

Updated
17 minutes ago

AppConnect Custom Configuration

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aas_min_allowed_auth_mode</td>
<td>modern_auth</td>
</tr>
<tr>
<td>email_watermark</td>
<td>$NULL$</td>
</tr>
<tr>
<td>show_dialing_confirmation</td>
<td>true</td>
</tr>
<tr>
<td>allow_detail_notifications</td>
<td>false</td>
</tr>
<tr>
<td>gai_search_display_name</td>
<td>true</td>
</tr>
<tr>
<td>default_network_timeout</td>
<td>90</td>
</tr>
<tr>
<td>email_password</td>
<td>$PASSWORD$</td>
</tr>
<tr>
<td>allow_export_contacts</td>
<td>true</td>
</tr>
<tr>
<td>email_alert_unsafe_domains</td>
<td>false</td>
</tr>
<tr>
<td>allow_logging</td>
<td>false</td>
</tr>
<tr>
<td>disable_analytics</td>
<td>true</td>
</tr>
<tr>
<td>email_exchange_host</td>
<td></td>
</tr>
<tr>
<td>email_max_attachment</td>
<td>10</td>
</tr>
<tr>
<td>email_safe_domains</td>
<td>$NULL$</td>
</tr>
<tr>
<td>email_ssl_required</td>
<td>true</td>
</tr>
<tr>
<td>email_watermark_parameters</td>
<td>#1:18888888.39.78.70</td>
</tr>
<tr>
<td>migrate_from_email_exchange_host</td>
<td>nnil</td>
</tr>
<tr>
<td>email_max_sync_period</td>
<td>0</td>
</tr>
<tr>
<td>email_default_sync_period</td>
<td>2</td>
</tr>
<tr>
<td>email_address</td>
<td></td>
</tr>
<tr>
<td>email_exchange_username</td>
<td></td>
</tr>
<tr>
<td>contacts_display_order</td>
<td>first_last</td>
</tr>
<tr>
<td>gai_search_minimum_characters</td>
<td>4</td>
</tr>
<tr>
<td>email_trust_all_certificates</td>
<td>false</td>
</tr>
<tr>
<td>prompt_email_password</td>
<td>false</td>
</tr>
<tr>
<td>show_pictures_default</td>
<td>false</td>
</tr>
<tr>
<td>allow_export_contacts_to_email</td>
<td>true</td>
</tr>
<tr>
<td>limit_contact_export_to</td>
<td>all</td>
</tr>
<tr>
<td>email_device_id</td>
<td>$DEVICE_UUID_NO_DASHES$</td>
</tr>
<tr>
<td>modern_auth_authority_url</td>
<td></td>
</tr>
<tr>
<td>modern_auth_resource_url</td>
<td></td>
</tr>
</tbody>
</table>

AppConnect Certificate Configuration
For more information on adding an application on Cloud, see "Adding an In-house app" in the Cloud Administrator Guide.

**KVPs for Email+ configuration**

- eas_min_allowed_auth_mode: modern_auth
- modern_auth_authority_url: https://<SentryHostname>/proxyservice
- modern_auth_resource_url: https://<SentryHostname>
- email_exchange_host = <sentry_address>
Standalone Sentry for AppTunnel

About Standalone Sentry for AppTunnel

Standalone Sentry configured for AppTunnel provides users secure access from an app on their device to your company’s backend resource such as a SharePoint server. AppTunnel protects app data-in-motion by providing app-by-app session security between an app and the corporate resource.

You configure Standalone Sentry for AppTunnel in the UEM. AppTunnel is part of a Tunnel deployment or an AppConnect app deployment.

Deploying AppTunnel is a two-step process:

1. In the UEM configure a Standalone Sentry for AppTunnel.
2. Configure one of the following for apps:
   - Configure an AppConnect app.
   Or
   - Configure Tunnel.

Before you configure Standalone Sentry for AppTunnel

1. You must have installed Standalone Sentry. See the Standalone Sentry Installation Guide.
2. If your UEM is Cloud, the Standalone Sentry must be registered to your Cloud instance.
3. You must have the required certificate setup in your UEM.

AppTunnel uses either an Identity certificate for device authentication and pass through or Kerberos for server authentication. The Identity certificate can be local or a trusted CA. If you are using an Identity certificate, you will upload the identity certificate in the Sentry configuration you create on your UEM. See "Configuring authentication using SCEP Identity (Cloud only)" on the next page.

Related topics

- "About Standalone Sentry for AppTunnel" above
- "Configuring Standalone Sentry for AppTunnel" on the next page
Configuring authentication using SCEP Identity (Cloud only)

For Cloud only, if you intend to use a SCEP identity certificate you must add the Certificate to Cloud and create the associated App Identity Certificate configuration.

**Procedure**

1. Add a local or external certificate authority in Admin > Certificate Authority. A Connector installation is required if you are using an external certificate authority.
2. Add an App Identity Certificate Configuration. For source, select the certificate you configured in Admin > Certificate Authority. This is the SCEP identity you will use when you configure device authentication in the Standalone Sentry configuration.
3. Create an Identity Certificate setting, in Configurations > Add > Identity Certificate. For Certificate Distribution, select Dynamically Generated and for Source, select the certificate you configured in Admin > Certificate Authority. If the app configuration requires, you will reference the Identity Certificate configuration in the app’s configuration that uses an AppTunnel service or the Tunnel service.

**Configuring Standalone Sentry for AppTunnel**

If you configure AppTunnel on a Standalone Sentry that was already configured for ActiveSync, and you change the device authentication options, ensure that the associated Exchange profile matches the device authentication options.

**Procedure**

1. In Cloud, go to Admin > Sentry.
2. Click +Add Sentry Profile or click on an existing profile to Edit.
3. Depending on the device authentication you will configure, select one of the following:
   - ActiveSync and/or App Tunnel with certificates
   - ActiveSync and/or App Tunnel with Kerberos
4. Use the guidelines provided in the following sections to configure Standalone Sentry for AppTunnel.
   - "Standalone Sentry connectivity global settings" below
   - "Device Authentication" below
   - "Default unmanaged devices behavior" below
   - "Passive health check options" on the next page
   - "Scheduling options" on the next page
   - "Default HTTP/TCP timeouts" on the next page
   - "Sentry server configuration" on the next page
   - "Advanced Traffic Control and server-side explicit proxy" on the next page
   - "AppTunnel service" on page 55

5. Click Save.

6. Assign the profile to a registered Standalone Sentry.
   Only one profile can be assigned to a Standalone Sentry.

Standalone Sentry connectivity global settings

See "Configuring Standalone Sentry connectivity settings" on page 23.

Device Authentication

Device authentication determines how users attempting to connect to the ActiveSync server or backend resource authenticate with Standalone Sentry. AppTunnel setup requires an Identity certificate or a Kerberos setup.

See "Device and server authentication" on page 60 for information on selecting and configuring a method of device authentication.

Default unmanaged devices behavior

By default, Sentry blocks unregistered devices from accessing backend resources.

See "Default unmanaged devices behavior" on page 24.
Passive health check options

These settings determine when a server is marked as ‘dead’.


Scheduling options

The options provide additional flexibility in managing multiple Sentrys.

See "Scheduling options" on page 25.

Default HTTP/TCP timeouts

WARNING: Do not make changes to the settings unless specifically instructed in the documentation or by Professional Services.

See "Default HTTP/TCP timeouts" on page 25.

Sentry server configuration

Configure the Sentry port, certificate, protocols and cipher suites.

See "Sentry server configuration" on page 26.

Advanced Traffic Control and server-side explicit proxy

- "Advanced traffic control" below
- "Server-side explicit proxy" on the next page

Advanced traffic control

Advance Traffic Control (ATC) allows you to manage access to backend resources based on which app the traffic is coming from and the destination IP address or domain name. ATC provides administrators additional control and flexibility in how traffic to backend resources are managed. You can specify whether traffic to the backend resource is through a proxy server, allowed direct access, or blocked.

Example: You may want to direct Safari traffic to go through a certain proxy server and all other traffic to go directly to backend resources. In this case, you would configure the Safari bundle ID in the Application BundleID and select the proxy server to direct Safari traffic, and set the Default Action to Allow.
If you are using a Standalone Sentry version 8.5.0 or earlier and configure ATC rules, Standalone Sentry will ignore the ATC rules.

<table>
<thead>
<tr>
<th>Rule type</th>
<th>App - Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-based rule</td>
<td>• Tunnel for Android and Windows.</td>
</tr>
<tr>
<td>Domain-based rule</td>
<td>• Tunnel for iOS</td>
</tr>
<tr>
<td></td>
<td>• AppConnect apps for iOS and Android devices.</td>
</tr>
<tr>
<td></td>
<td>• SharePoint for Docs@Work</td>
</tr>
<tr>
<td></td>
<td>• CIFS for Docs@Work</td>
</tr>
<tr>
<td></td>
<td>• Web@Work</td>
</tr>
</tbody>
</table>

**Server-side explicit proxy**

Standalone Sentry supports sending traffic through an HTTP proxy server to access corporate resources. The proxy server is located behind the firewall and sits between the Sentry and corporate resources. This deployment allows you to access corporate resources without having to open the ports that Sentry would otherwise require.

Consider the following:

- This configuration is only supported for AppTunnel traffic.
- Proxy is configured for each AppTunnel service. You may configure proxy for some AppTunnel services and not for other AppTunnel services on the same Sentry.
- The same proxy server may be configured on multiple Sentrys.

Standalone Sentry filters HTTP traffic through a TCP tunnel that uses server-side explicit proxy. For HTTP traffic through a TCP tunnel, if server-side explicit proxy is configured, Standalone Sentry will treat the explicit proxy as HTTP proxy. The HTTP request URL will be modified to include the target host.

In all other cases, Standalone Sentry treats the explicit proxy server as a TCP proxy server. Sentry will send a HTTP CONNECT request to the explicit proxy, followed by TCP data.
TABLE 2. FIELD DESCRIPTIONS FOR ADVANCED TRAFFIC CONTROL (ATC)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Traffic Control</td>
<td>Select to enable advanced traffic control.</td>
</tr>
<tr>
<td><strong>Server-side Proxy List</strong></td>
<td>Traffic is directed to the proxy servers listed here based on the backend resource and action defined in Traffic Control Rules.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for the proxy server. The name for the proxy server will be available for selection in the Proxy field for Traffic Control Rules.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the IP address or FQDN for the proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for the proxy server.</td>
</tr>
<tr>
<td>+</td>
<td>Click to add a proxy server.</td>
</tr>
</tbody>
</table>

**Traffic control rules**

Specify whether traffic from an app to the backend resource is through a proxy server, allowed direct access, or blocked. You can create multiple rule sets. Each rule set can have multiple rules. However, all rules in a rule set can only be one type, either IP based or domain based. You cannot create a mix of IP based and domain based rules in a rule set.

Note The Following:

- Rules in a rule set are matched based on the order in which they are listed. This is especially important for domain names with wildcards. For example, if the Block action is selected for *.company.com, and the Proxy action is selected for *.internal.company.com, and the rule for *.company.com is listed first, then all company.com domains will be blocked. Use the up and down arrows to order the rules.

- If AppTunnel traffic is blocked due to traffic control rules, the AppTunnel entry is not reported in the Sentry tab in device details for a device.

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Select one of the following:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• IP based: The rule is matched based on the IP address of the destination host. IP based rules are supported only for IP traffic from Windows and Android devices going through Tunnel. The destination has to be an IP address or an IP range. Example: 10.0.0.0/8, 10.5.0.0/16, 10.5.2.0/24, 10.5.5.2/32</td>
</tr>
</tbody>
</table>
### TABLE 2. FIELD DESCRIPTIONS FOR ADVANCED TRAFFIC CONTROL (ATC) (Cont.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Domain based: The rule is matched based on the domain of the destination host and the bundle ID of the app. Domain based rules are supported only for HTTP/S and TCP traffic from iOS devices going through Tunnel. The destination has to be a domain name.</td>
</tr>
<tr>
<td>Destination Host</td>
<td>Enter the IP address or domain name of the backend resource:</td>
</tr>
<tr>
<td></td>
<td>- IP based rules: Enter an IP address or range. The IP address range must conform CIDR format. Example: 192.168.0.15/24</td>
</tr>
<tr>
<td></td>
<td>- Domain based rules: Port numbers are not supported. Wildcards are supported. Only the suffix after the * wildcard is matched. Example: *.acme.com.</td>
</tr>
<tr>
<td>Application Bundle ID</td>
<td>Enter the app bundle ID for which you are creating the domain-based rule. The bundle ID can include &quot;*&quot; for wildcard matching. The bundle ID can be used in conjunction with Destination Host. If you are using the bundle ID with a destination host, then the rule will be applied only to traffic from the app directed to the destination host.</td>
</tr>
<tr>
<td>Action</td>
<td>Select <strong>Proxy</strong>, <strong>Allow</strong>, or <strong>Block</strong>.</td>
</tr>
<tr>
<td>Proxy</td>
<td>If you selected <strong>Proxy</strong> for <strong>Action</strong>, then select the proxy server for the backend resource.</td>
</tr>
<tr>
<td>Default Action</td>
<td>The default action is applied if traffic control rules is not defined for a backend resource.</td>
</tr>
<tr>
<td>Proxy</td>
<td>If you choose <strong>Proxy</strong> as the default action, select the proxy server for traffic to the backend resource.</td>
</tr>
</tbody>
</table>

### AppTunnel service

Select one of the app services to create an AppTunnel service for that app.

- "Service types and supported traffic" on the next page
- "Field description for AppTunnel service" on the next page
- "About context headers" on page 58
Service types and supported traffic

The following table describes the service type available when configuring AppTunnel and the traffic type supported by the service.

<table>
<thead>
<tr>
<th>Service type</th>
<th>Supports traffic type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharepoint for Docs@Work</td>
<td>• iOS: HTTP, HTTPS</td>
</tr>
<tr>
<td></td>
<td>• Android: HTTP, HTTPS</td>
</tr>
<tr>
<td>CIFS for Docs@Work</td>
<td>• iOS: CIFS</td>
</tr>
<tr>
<td></td>
<td>• Android: CIFS</td>
</tr>
<tr>
<td>Web@Work</td>
<td>• iOS: HTTP, HTTPS</td>
</tr>
<tr>
<td></td>
<td>• Android: HTTP, HTTPS</td>
</tr>
<tr>
<td>Tunnel</td>
<td>• iOS: HTTPS, TCP, IP (split tunneling for UDP traffic)</td>
</tr>
<tr>
<td></td>
<td>• Windows: HTTPS, TCP, IP (including UDP).</td>
</tr>
<tr>
<td></td>
<td>• Android: HTTPS, TCP, IP (including UDP).</td>
</tr>
<tr>
<td>Help@Work</td>
<td>• iOS: TCP (includes HTTP and HTTPS)</td>
</tr>
<tr>
<td>Custom HTTP</td>
<td>• HTTP and HTTPS</td>
</tr>
<tr>
<td></td>
<td>• Any service other than TCP and IP</td>
</tr>
<tr>
<td>Custom TCP</td>
<td>• TCP</td>
</tr>
</tbody>
</table>

Field description for AppTunnel service

The following table describes the fields available for configuring an AppTunnel service. The fields available for configuration changes depending on the type of service you are configuring.
### TABLE 4. FIELD DESCRIPTIONS FOR APP TUNNEL SERVICE

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The <strong>Service Name</strong> identifies the AppTunnel service. The service name is referenced in the AppConnect app configuration for configuring tunneling for the AppConnect app. The app is restricted to accessing the backend resources listed in the <strong>Server List</strong> field. A service name cannot contain these characters: 'space' \ * ? &lt; &quot;</td>
</tr>
<tr>
<td>Service Type (only Tunnel iOS or Mac)</td>
<td>IP: Select to configure packet-tunnel provider type VPN. TCP: Select to configure app-proxy VPN.</td>
</tr>
<tr>
<td>Enable DFS</td>
<td>Select the check box if you are configuring a DFS site in Docs@Work. Only for Docs@Work for CIFS service.</td>
</tr>
<tr>
<td>Server Authentication</td>
<td>Select the authentication scheme for the Standalone Sentry to use to authenticate the user to the backend resource:</td>
</tr>
<tr>
<td></td>
<td>- Pass through (Basic Authentication)</td>
</tr>
<tr>
<td></td>
<td>The Sentry passes through the authentication credentials, such as the user ID and password (basic authentication) or NTLM, to the backend resource.</td>
</tr>
<tr>
<td></td>
<td>NOTE: For TCP and IP tunneling, select Pass Through. The Sentry passes through all TCP or IP packets to the backend resource.</td>
</tr>
<tr>
<td></td>
<td>- Kerberos</td>
</tr>
<tr>
<td></td>
<td>The Sentry uses Kerberos Constrained Delegation (KCD). KCD supports Single Sign On (SSO). SSO means that the device user does not have to enter any credentials when the AppConnect app accesses the backend resource.</td>
</tr>
<tr>
<td></td>
<td>The Kerberos option is only available if:</td>
</tr>
<tr>
<td></td>
<td>- You selected ActiveSync and/or App Tunnel with Kerberos.</td>
</tr>
<tr>
<td></td>
<td>- Kerberos authentication is now supported with Exchange ActiveSync, Web@Work, SharePoint for Docs@Work, and CIFS for Docs@Work services.</td>
</tr>
<tr>
<td></td>
<td>If you select Kerberos, additional fields are displayed. See &quot;Authentication using an Identity certificate and Kerberos constrained delegation&quot; on page 64.</td>
</tr>
</tbody>
</table>
### Table 4. Field Descriptions for AppTunnel Service (Cont.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All destinations (forward proxy)</td>
<td>Select if you want all traffic from the app to go through Standalone Sentry.</td>
</tr>
<tr>
<td>Specific destinations (reverse proxy)</td>
<td>Select if you want to restrict traffic to only specific servers. Standalone Sentry sends through only requests to the configured servers.</td>
</tr>
</tbody>
</table>
| Servers (reverse proxy) | Add the backend resource’s fully qualified domain name (FQDN) and port number on the backend resource that the Sentry can access.  
Example: `sharepoint1.companyname.com:443`  
Acceptable characters in a host name are letters, digits, and a hyphen. The name must begin with a letter or digit.  
You can enter multiple resources. The Sentry uses a round-robin distribution to load balance. That is, it sets up the first tunnel with the first resource, the next with the next resource, and so on. |
| Enable Server TLS | Select **Enable Server TLS** if the servers listed in the **Servers** field require SSL.  
> **i** Although port 443 is typically used for https and requires SSL, the backend resource can use other port numbers requiring SSL. |
| ATC Rule Set | Select the ATC rule set if you want to manage the AppTunnel service traffic through ATC rules.  
You must also have configured Advanced Traffic Control (ATC) rules. Only the rule type supported by the app will be listed. |
| Add Context Headers | Select the check box to forward additional device context information to your corporate backend resource.  
This allows your corporate backend resources to further validate the device.  
> **i** Context headers are not supported for TCP tunneling. |

### About context headers

As an administrator you may require your corporate backend resources to further validate the devices accessing these resources. In these cases, Standalone Sentry forwards context information in the header. You enable context headers in a service configuration. So, you can decide to enable context headers for some services and not enable context headers for other services.
If server-side explicit proxy is configured, the request to the proxy (HTTP CONNECT) includes the context headers.

### TABLE 5. INFORMATION IN CONTEXT HEADERS

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-MobileIron-DEVICE-UUID</td>
<td>Device UUID&lt;br&gt;The Device UUID can be used in API calls to Cloud to collect more information about the device.</td>
</tr>
<tr>
<td>X-MobileIron-USER-UPN</td>
<td>User Principal name</td>
</tr>
<tr>
<td>X-MobileIron-USER-DN</td>
<td>User DN (if available)</td>
</tr>
<tr>
<td>X-MobileIron-USER-CERT</td>
<td>User Identity certificate&lt;br&gt;The certificate is represented in a Privacy Enhanced Mail (PEM) encoding without the header or the trailer information.</td>
</tr>
</tbody>
</table>

### Configuring apps

After configuring AppTunnel on Standalone Sentry, configure the apps to use AppTunnel. See the following documents for information on configuring apps:

### TABLE 1. DOCUMENTATION REFERENCE

<table>
<thead>
<tr>
<th>Product</th>
<th>Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>Cloud Guide or Help documentation.</td>
</tr>
<tr>
<td>Email+</td>
<td>Email+ for iOS Guide for Administrators.&lt;br&gt;Email+ for Android Guide for Administrators.</td>
</tr>
<tr>
<td>Docs@Work</td>
<td>Docs@Work for iOS Guide for Administrators.&lt;br&gt;Docs@Work for Android Guide for Administrators.</td>
</tr>
</tbody>
</table>
Device and server authentication

Overview

Standalone Sentry supports device authentication using user name and password, certificate-based authentication, or Kerberos Constrained Delegation. Device authentication involves configuring:

- device authentication (how the device authenticates to the Standalone Sentry)
- server authentication (how the Standalone Sentry authenticates the device to the server).

Device authentication

Device authentication specifies how the device authenticates to the Standalone Sentry. The following table describes the devices authentication methods supported by Standalone Sentry.

<table>
<thead>
<tr>
<th>Device Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass Through</td>
<td>Only available if you are using the Sentry for ActiveSync only. The Sentry passes through the authentication provided by the device, for example, user name and password, NTLM.</td>
</tr>
<tr>
<td>Group Certificate</td>
<td>Available for ActiveSync and AppTunnel. Requires the following:</td>
</tr>
<tr>
<td></td>
<td>• A trusted group certificate for device authentication.</td>
</tr>
<tr>
<td></td>
<td>• A authentication method like user name and password or NTLM for authenticating the device to the server.</td>
</tr>
<tr>
<td>Identity Certificate</td>
<td>Available for ActiveSync and AppTunnel. Requires the following:</td>
</tr>
</tbody>
</table>

KCD is not supported with Group Certificates.
### Server authentication

Server authentication specifies how the Sentry authenticates the device to the backend resource. This can be the ActiveSync server or a backend resource. The following table describes the supported server authentication. These are supported for both ActiveSync and AppTunnel.

**Table 2. Supported server authentication**

<table>
<thead>
<tr>
<th>Server Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass Through</td>
<td>The Sentry passes through the authentication provided by the device. For example: user name and password, NTLM.</td>
</tr>
<tr>
<td></td>
<td>This is the only authentication option you can use with Microsoft Office 365. This is also the only authentication option available for TCP and IP tunneling.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Only available if you choose Identity Certificate for device authentication. Requires a properly configured Kerberos implementation.</td>
</tr>
</tbody>
</table>

### Configuring device and server authentication

You specify the device and server authentication in the Sentry configuration when you create a Sentry profile in Admin > Sentry. Click **Add Sentry Profile** or edit an existing Sentry profile.

Select one of the following:

- **ActiveSync with basic auth**: Only for Sentry for ActiveSync. Sentry passes through the user name and password provided by the device user.
- **ActiveSync and/or AppTunnel with certificates**: Select if you plan to use Identity certificates (X.509) for device authentication. Pass through is the only option available for server authentication.

- **ActiveSync and/or App Tunnel with Kerberos**: Select if you plan to use Kerberos to authenticate the device to the server.

If you do device authentication with Identity certificates, you can specify different server authentication types for the ActiveSync configuration and for each AppTunnel service. For example, you can specify Pass Through for the ActiveSync server and Kerberos Constrained Delegation (KCD) for the servers listed for an AppTunnel service.

**Procedure**

1. Obtain the certificates required for your implementation.
2. In Admin > Sentry, click Add Sentry Profile or edit an existing Sentry profile.
3. For Authentication select one of the following authentication options, depending on your implementation:
   - **ActiveSync with basic auth**
     See "ActiveSync with basic auth and pass through" below for next steps.
   - **ActiveSync and/or AppTunnel with group certificates**
     See "Authentication using a group certificate and pass through" below for next steps.
   - **ActiveSync and/or AppTunnel with Identity Certificate**
     See "Authentication using a SCEP Identity certificate and pass through" on the next page for next steps.

   OR

   See "Authentication using an Identity certificate and Kerberos constrained delegation" on page 64 for next steps.

**ActiveSync with basic auth and pass through**

If you select **ActiveSync with basic auth** for authentication, then Standalone Sentry passes through the user name and password provided by the device user. No additional configuration on Cloud is required.

**Authentication using a group certificate and pass through**

If you select **ActiveSync and/or AppTunnel with certificates**, additional configuration fields display for **Authentication**.

For device authentication with group certificate, **Pass Through** is the only option available for server authentication.

To complete the configuration:

1. In the Standalone Sentry profile with **ActiveSync and/or AppTunnel with certificates**, in **Global Settings**, for **Device Authentication Mode**, select **Use a single certificate for 2-factor auth (basic + cert)**.
2. Click **Upload Certificate**.
   Additional fields are displayed.
3. Enter the **Certificate name** and **Password** for the certificate.
4. Upload the certificate (usually a .cer or PKCS 12 file) you trust.
5. Click **Save**.

**NOTE:** Though certificate is uploaded, it does not persist until you click **Save**.
6. If you want to validate the certificates presented by the device against the Certificate Revocation List (CRL) published by the CA, then select **Check Certificate Revocation List (CRL)**.

**NOTE:**
- CRL check should be enabled only if the certificate chain presented by the device or the Trusted-Front-End to Standalone Sentry contains information to download CRL over HTTP.
- Only HTTP- and HTTPS-based CRLs are supported. Some CAs create LDAP-based CRLs by default that will not work with Sentry.
- For CRL validation to work, Sentry requires network connectivity to the CRL Distribution Point (CDP), usually the CA that issued the certificate, through an HTTP or HTTPS port.
7. **Server Authentication** defaults to **Pass Through** in any service, ActiveSync or AppTunnel, that you configure.
8. Click **Save**.
   The Sentry restarts.

### Authentication using a SCEP Identity certificate and pass through

If you select **ActiveSync and/or AppTunnel with certificates**, additional configuration fields display for **Authentication**. This section describes the configuration when you choose **Use SCEP Identity** to authenticate the device to the Sentry and Sentry uses **Pass Through** for authenticating the device to the ActiveSync server or a backend resource.

**Before you begin**

You must have completed the steps described in "Configuring authentication using SCEP Identity (Cloud only)" on page 50.

**Procedure**

1. In the Standalone Sentry profile with **ActiveSync and/or AppTunnel with certificates**, in **Global Settings**, for **Device Authentication Mode**, select **SCEP Identity**.
2. Select the **App Identity Certificate Configuration** for the Identity certificate you want devices to use to authenticate with Sentry.
3. If you want to validate the certificates presented by the device against the Certificate Revocation List (CRL) published by the CA, then select **Check Certificate Revocation List (CRL)**.

**NOTE:**
- CRL check should be enabled only if the certificate chain presented by the device or the Trusted-Front-End to Standalone Sentry contains information to download CRL over HTTP.
- Only HTTP- and HTTPS-based CRLs are supported. Some CAs create LDAP-based CRLs by default that will not work with Sentry.
- For CRL validation to work, Sentry requires network connectivity to the CRL Distribution Point (CDP), usually the CA that issued the certificate, through an HTTP or HTTPS port.

4. **Server Authentication** defaults to **Pass Through** in any service, ActiveSync or AppTunnel, that you configure.
5. Click **Save**.
   The Sentry restarts.

**Authentication using an Identity certificate and Kerberos constrained delegation**

This section describes the configuration when you choose **Identity Certificate** to authenticate the device to the Sentry and **Kerberos** for how Sentry authenticates the device to the ActiveSync server or backend resource.

Note The Following:

- For ActiveSync, Sentry supports Kerberos authentication only with Microsoft Exchange Servers.
- If you are configuring tunneling to a DFS server, in the Kerberos distribution center, map the SPN of the CIFS service domain to one of its domain controllers. See "Configuring Kerberos authentication for DFS" on page 66.
- Kerberos initialization in Standalone Sentry occurs only during tomcat start up. Standalone Sentry obtains the ticket-granting ticket (TGT) during Kerberos initialization. If the initialization fails during tomcat start up, Standalone Sentry automatically continues to retry until a service ticket from the KDC is received. The retry interval starts at one minute and maxes out at one-hour intervals. Failed initialization attempts are reported with a WARN level log in Standalone Sentry System Manager in Monitoring. To manually initialize Kerberos, use the debug command, debug sentry kerberos init. The command has no impact if Kerberos initialization has already been completed.

**Before you begin**

You must have set up your Kerberos environment. See **Authentication Using Kerberos Constrained Delegation** on the Support site.

The **Authentication Using Kerberos Constrained Delegation document** has setup instruction on Core also. Please ignore the setup instruction for Core.

**Procedure**

1. In the Standalone Sentry profile with **ActiveSync and/or AppTunnel with Kerberos**, in **Global Settings**, for **Device Authentication Mode**, select **Use SCEP Identity**.
2. Select the **App Identity Certificate Configuration** for the Identity certificate you want devices to use to authenticate with Sentry.
3. If you want to validate the certificates presented by the device against the Certificate Revocation List (CRL) published by the CA, then select **Check Certificate Revocation List (CRL)**.

**NOTE:**
- CRL check should be enabled only if the certificate chain presented by the device or the Trusted-Front-End to Standalone Sentry contains information to download CRL over HTTP.
- Only HTTP- and HTTPS-based CRLs are supported. Some CAs create LDAP-based CRLs by default that will not work with Sentry.
- For CRL validation to work, Sentry requires network connectivity to the CRL Distribution Point (CDP), usually the CA that issued the certificate, through an HTTP or HTTPS port.

4. In the Kerberos section, add Realm and Key Distribution Center (KDC).
   - **Realm:** The Kerberos administrative domain with CIFS sahres. The realm is usually the company domain name, in all uppercase characters.
   - **Key Distribution Center:** The Key Distribution Center is the network service that supplies session tickets and temporary session keys. This is generally the Active Directory domain controller host name.

5. Click **Next** to enter or update Sentry Server Configuration information.
6. Click **Next** to add or edit a service and configure server authentication.
7. For **Server Authentication** for a service, ActiveSync or AppTunnel that you configure, select **Kerberos**. When you select **Kerberos** for **Server Authentication**, **Specific destinations (reverse proxy)** is selected by default. The **Derive Service Principal Name (SPN) from fully qualified Server Name** option appears.
   If you select **All Destinations (forward proxy)**, the **Certificate Field Mapping** section also appears. Click + **Add** to add an entry for certificate mapping.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derive Service Principal Name (SPN) from fully qualified Server Name</td>
<td>Select to derive the Service Principal Name of the KCD from the FQDN of the ActiveSync server. When you select forward proxy, SPN is automatically derived from the FQDN of the ActiveSync server. Therefore, this option is not available when you select forward proxy.</td>
</tr>
</tbody>
</table>
| Certificate Field Mapping | Specify the certificate fields that Standalone Sentry can use to derive users’ UPN and Realm for Kerberos authentication.  
  a. Select the field from which Standalone Sentry will derive the User UPN or User DN.  
  **NOTE:** For WP8.1 devices, for User UPN, select either **DNS Name** or **RFC 822 Name**, and for User DN select **Certificate Subject**.  
  b. For each corresponding field selected, select **User UPN** or **User DN**.  
  **NOTE:** This field is required in a cross-realm Kerberos environment. |

8. If you selected reverse proxy, then you must also add the FQDN and port for the allowed servers. This must be the FQDN of the backend resource. Wildcards are not supported. If you did not select **Derive Service Principal Name (SPN) from fully qualified Server Name**, then you must also add the SPN.
9. Click **Next**, then Click **Save**
Standalone Sentry restarts when the profile is pushed to Standalone Sentry.

Cross-realm Kerberos support

Support for cross-realm Kerberos on the Standalone Sentry is enabled by default, and does not require any actions from the administrator.

Cross-realm S4U2Self is supported. Cross-realm S4U2Proxy is not supported.

Configuring Kerberos authentication for DFS

Authentication to DFS servers using Kerberos requires additional setup in the KDC and the Standalone Sentry system manager. To support Kerberos authentication for DFS, map the SPN of the CIFS service domain to one of its domain controllers (DC). If your Kerberos environment has multiple domain controllers (DC), to avoid authentication failure, add the DC you are mapping to as a static host in the Standalone Sentry system manager.

If your Kerberos environment has multiple domain controllers (DC), note that you can only map the SPN of the CIFS service domain to one DC.

Before you begin

Setup Standalone Sentry for authentication using Kerberos. See "Authentication using an Identity certificate and Kerberos constrained delegation" on page 64

Procedure

1. Map the SPN of the domain to one of its Domain Controllers (DC).
2. On the KDC, associate the Standalone Sentry service account to the CIFS service.
3. If the domain contains multiple DCs, add a static host for the DC in the Standalone Sentry system manager:
   a. Sign in to the Standalone Sentry system manager.
   b. Go to Settings > Static Hosts.
   c. Click Add.
   d. Configure the following:
      IP address: IP address of the DC.
      FQDN: FQDN of the DC entered in Step 1.
      Alias: short name of DC followed by space.
      Example:
      IP Address: 192.168.10.5
      FQDN: win2k8.texas.enterprise.com
      Alias: win2k8 texas.enterprise.com
   e. Click Save.
Related topics

- "Static Hosts" on page 79.
Working with connections through Standalone Sentry

Standalone Sentry connections on Cloud ................................................................. 68
Connections from managed devices ................................................................. 68
Unmanaged connections .................................................................................... 70

Standalone Sentry connections on Cloud

Devices connecting to backend resources through Standalone Sentry can be managed (registered with Cloud) or unmanaged (not registered with Cloud).

A record of users attempting to connect from managed devices is provided in Devices > Devices. A record of the users attempting to connect from unmanaged devices is provided in Devices > Unmanaged Connections.

Related topics

• "Connections from managed devices" below.
• "Unmanaged connections" on page 70.

Connections from managed devices

Typically, devices register with a Cloud, which provides the devices with the configurations that allow users on the devices to access backend resources.

To view the users on managed devices that connect to your ActiveSync server or any other backend resource through Standalone Sentry, in Cloud, go to Devices, click on a device name, then click on the Sentry tab. Information displayed on this page is updated when Standalone Sentry syncs with Cloud.

Each unique combination of user (email account) on the device and app connecting to the backend resource displays as a separate record in the in the Sentry tab. If there are multiple accounts on the device, then each User is listed. If multiple apps are being used, then each app (User-Agent) is displayed as a separate record.

• "Information displayed in each record for a connection from a managed device" on the next page.
• "Taking action on a record for a connection from a managed device" on the next page.
Information displayed in each record for a connection from a managed device

The following table describes the information displayed for each record in the Cloud in Devices > Sentry.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The device user.</td>
</tr>
<tr>
<td>Sentry Hostname</td>
<td>The Standalone Sentry hostname through which the device is connecting with</td>
</tr>
<tr>
<td></td>
<td>the ActiveSync server or the backend resource.</td>
</tr>
<tr>
<td>User-Agent</td>
<td>The app connecting to the backend resource.</td>
</tr>
<tr>
<td></td>
<td>This could be the email app or any other app connecting to the ActiveSync</td>
</tr>
<tr>
<td></td>
<td>server or backend resource.</td>
</tr>
<tr>
<td>Version</td>
<td>The app version.</td>
</tr>
<tr>
<td>Bundle Id</td>
<td>Bundle Id of the app connecting to the backend resource.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the device is <strong>Allow</strong> or <strong>Block</strong>.</td>
</tr>
<tr>
<td></td>
<td>The status for a connection is blocked if the device is out of compliance.</td>
</tr>
<tr>
<td>Actions</td>
<td>Administrators can <strong>Allow</strong>, <strong>Block</strong>, or <strong>Delete</strong> a record.</td>
</tr>
</tbody>
</table>

Taking action on a record for a connection from a managed device

Actions applied on a Standalone Sentry connection record only impacts the user associated with the app in that record. The user using another app or the same user on another device is not impacted. The only action you can take on a record is delete.

Deleting a record removes the record from the list in Devices > Sentry. However, if the device attempts to connect to the backend resource

**Procedure**

1. In Cloud, go to Devices > Devices.
2. Click the name for a record.
3. Click on the Sentry tab.
4. Click **Delete** for the record you want to delete.
Unmanaged connections

Sometimes users can access backend resources through Standalone Sentry from devices that are not managed by Cloud. In these cases these connections are displayed in Devices > Unmanaged Connections.

Related topics

- "Information displayed in each record for a connection from an unmanaged device" below.
- "Taking action on a record for an unmanaged connection " on the next page.

Information displayed in each record for a connection from an unmanaged device

The following table describes the information displayed for each record in the Cloud in Devices > Unmanaged Connections.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The device user.</td>
</tr>
<tr>
<td>Connection Source</td>
<td>The device type from which the connection is made.</td>
</tr>
<tr>
<td>ActiveSync Id</td>
<td>ActiveSync Id of user connecting to the backend resource. Only connections to the ActiveSync server can be from unmanaged devices.</td>
</tr>
<tr>
<td>Override Action</td>
<td>Displays the Action taken on the unmanaged connection by the administrator. The actions displayed are Allow or Block.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the device is Allow or Block. The status for a connection is Allow if the Allow unmanaged devices to receive email and data setting is enabled or the connection was previously allowed by the administrator, and Block if it is disabled.</td>
</tr>
<tr>
<td>Created At</td>
<td>The date and time the connection was created.</td>
</tr>
<tr>
<td>Sentry Hostnames</td>
<td>The Standalone Sentry hostname through which the device is connecting with the ActiveSync server or the backend resource.</td>
</tr>
</tbody>
</table>

TABLE 1. INFORMATION DISPLAYED FOR CONNECTIONS FROM UNMANAGED DEVICES
Taking action on a record for an unmanaged connection

Actions applied on a Standalone Sentry connection record only impacts the user associated with the device in that record. The user using another app or the same user on another device is not impacted. You can take the following actions on connections from unmanaged devices:

- **Allow**: Apply the action on a record that was manually blocked or blocked by configuration. Allows the user on the device in the record to access the ActiveSync server.

- **Block**: Blocks the user on the device in the record from accessing the ActiveSync server.

- **Delete**: Deleting a record removes the record from the list. However, if the device attempts to connect to the backend resource it is allowed or blocked depending on whether the **Allow unmanaged devices to receive email and data** setting is enabled or disabled.

Procedure
1. In Cloud, go to Devices > Unmanaged Connections.
2. Select a record on which you want to take action.
3. Click Action and select the action to apply.
Standalone Sentry Settings

The following describe the Standalone Sentry settings in the Standalone Sentry System Manager:

Overview of Standalone Sentry settings ................................................................. 72
Interfaces .................................................................................................................. 73
Routes ....................................................................................................................... 76
DNS and Hostname ................................................................................................. 78
Static Hosts ............................................................................................................... 79
Date and Time (NTP) ............................................................................................. 81
CLI ............................................................................................................................. 82
Splunk ....................................................................................................................... 82
Syslog ....................................................................................................................... 84
SNMP ....................................................................................................................... 87
Email Settings ......................................................................................................... 92
Login ......................................................................................................................... 94
Timeout ..................................................................................................................... 95
Services ................................................................................................................... 96
Sentry ....................................................................................................................... 97
Incoming SSL configuration .................................................................................... 98
Outgoing SSL configuration ................................................................................... 98
UEM SSL Configuration .......................................................................................... 98
Access SSL Configuration ...................................................................................... 101
Outbound HTTP Proxy ........................................................................................... 104
Log representation and format ............................................................................. 105

Overview of Standalone Sentry settings

The settings tab in the Standalone Sentry System Manager contains links for configuring Standalone Sentry.

To log in to the Sentry System Manager, go to
https://fully_qualified_hostname:8443.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network: Interfaces</td>
<td>Change physical interface settings.</td>
</tr>
<tr>
<td></td>
<td>Add VLAN interfaces.</td>
</tr>
<tr>
<td></td>
<td>Change VLAN interfaces.</td>
</tr>
<tr>
<td>Network: Routes</td>
<td>Change the default gateway.</td>
</tr>
<tr>
<td></td>
<td>Route through different gateways.</td>
</tr>
<tr>
<td>DNS and Hostname</td>
<td>Change DNS servers.</td>
</tr>
<tr>
<td>Static Hosts</td>
<td>Edit the host list for the Standalone Sentry.</td>
</tr>
<tr>
<td>Date and Time (NTP)</td>
<td>Change the time source used by the Standalone Sentry.</td>
</tr>
<tr>
<td>CLI</td>
<td>Change the Enable Secret set during installation.</td>
</tr>
<tr>
<td></td>
<td>Enable or Disable ssh access.</td>
</tr>
<tr>
<td></td>
<td>Change ssh settings.</td>
</tr>
<tr>
<td>Splunk</td>
<td>Configure Splunk server.</td>
</tr>
<tr>
<td>Syslog</td>
<td>Configure Syslog servers.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Configure SNMP servers.</td>
</tr>
<tr>
<td>Email Settings</td>
<td>Configure SMTP servers.</td>
</tr>
<tr>
<td>Services</td>
<td>Enable or Disable Sentry services.</td>
</tr>
<tr>
<td>Services: Sentry</td>
<td>Allow or block New device access when UEM is unreachable.</td>
</tr>
</tbody>
</table>

**Interfaces**

The **Settings > Interfaces** screen enables you to change parameters for the network interface points for Standalone Sentry:

- physical and VLAN interfaces
- static routes

Physical and VLAN interface fields are not editable for a Standalone Sentry installed on Microsoft Azure. These are assigned by the Microsoft Azure infrastructure.
You configure a physical network interface as part of the installation process. You can use the Interfaces screen to:

- Edit the physical interface settings specified during installation
- Add physical interfaces
- Add VLAN interfaces
- Change VLAN interfaces

**Physical interface mapping to M2600 NIC ports**

The following table provides a mapping of the physical interface name in the Core System Manager to the physical NIC port in the M2600 appliance. The six Gigabit Ethernet interfaces are available only on an M2600 appliance.

<table>
<thead>
<tr>
<th>Physical interface</th>
<th>M2600 NIC port</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet1</td>
<td>I - eth0 (NIC-3)</td>
</tr>
<tr>
<td>GigabitEthernet2</td>
<td>J - eth1 (NIC-4)</td>
</tr>
<tr>
<td>GigabitEthernet3</td>
<td>K - eth2 (NIC-5)</td>
</tr>
<tr>
<td>GigabitEthernet4</td>
<td>L - eth3 (NIC-6)</td>
</tr>
<tr>
<td>GigabitEthernet5</td>
<td>C - eth4 (NIC-1)</td>
</tr>
<tr>
<td>GigabitEthernet6</td>
<td>D - eth5 (NIC-2)</td>
</tr>
</tbody>
</table>

**Changing physical interfaces**

You can change the physical interfaces for Standalone Sentry in the Sentry System Manager.

**Procedure**

1. Click the interface name.
**Figure 1. Modify Physical Interfaces**

![Modify Interface](image1)

2. Change any or all of the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Enter the IP address of the physical network interface. Unless you are configuring a standalone implementation for a small trial, you should specify at least one physical interface.</td>
</tr>
<tr>
<td>Mask</td>
<td>Enter the netmask of the physical network interface.</td>
</tr>
<tr>
<td>ACL Name</td>
<td>Select an Access Control List for this interface.</td>
</tr>
<tr>
<td>Admin State</td>
<td>To enable this interface for use with the system, click Enable. To temporarily prevent use of this interface with the system, click Disable.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

**Adding VLAN interfaces**

Virtual Local Area Network (VLAN) interfaces are optional interfaces you can configure on UEM to manage bandwidth and load balancing. You can add a VLAN interface in the Standalone Sentry System Manager.

**Procedure**

1. Click **Add VLAN**.

**Figure 2. Adding VLAN**

![Add VLAN](image2)
2. Use the following guidelines to complete the configuration:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>Specify a number between 2 and 4094.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address for this VLAN interface.</td>
</tr>
<tr>
<td>Mask</td>
<td>Enter the netmask for this VLAN interface.</td>
</tr>
<tr>
<td>Physical Interface</td>
<td>Select the physical interface that corresponds to this VLAN interface.</td>
</tr>
<tr>
<td>ACL Name</td>
<td>Select an Access Control List for this interface. See &quot;Access Control Lists&quot; on page 119.</td>
</tr>
<tr>
<td>Admin State</td>
<td>To enable this interface, click Enable. To temporarily suspend use of this VLAN, click Disable.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

**Deleting a VLAN interface**

You can delete the Standalone Sentry Virtual Local Area Network (VLAN) interface in the Sentry System Manager.

**Procedure**
1. Select the VLAN you want to remove.
2. Click **Delete VLAN**.

**Routes**

The **Settings > Network > Routes** screen enables you to create and maintain static network routes within the enterprise.
Adding network routes

You can add network routes in the Standalone Sentry System manager in Settings > Network > Routes.

**Procedure**

1. In the Standalone Sentry System Manager go to Settings > Network > Routes.
2. Click Add.

**Figure 2. Adding network routes**

3. Use the following guidelines to complete the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Enter the network IP address.</td>
</tr>
<tr>
<td>Mask</td>
<td>Enter the subnet mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the IP address for the gateway.</td>
</tr>
</tbody>
</table>

4. Click Save.
Deleting network routes

You can delete the network routes in the Standalone Sentry System manager.

Procedure
1. In the Standalone Sentry System Manager go to Settings > Network > Routes.
2. Select the entry.
3. Click Delete.

DNS and Hostname

The DNS and Hostname screen displays the hostname, default domain, and DNS information entered during installation. Use this screen to:

- Change the hostname
- Change the default domain
- Change or add DNS servers

DNS and hostname fields are not editable for a Standalone Sentry installed on Microsoft Azure. These are assigned by the Microsoft Azure infrastructure.

The following table describes the fields for DNS and hostname.
**Table 1. DNS and Hostname Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Specify the fully-qualified host name for the appliance.</td>
</tr>
<tr>
<td>Default Domain</td>
<td>Specify the default domain for the appliance.</td>
</tr>
<tr>
<td>Preferred DNS Server</td>
<td>Specify the IP address of the primary DNS server to use.</td>
</tr>
<tr>
<td>Alternate DNS Server 1</td>
<td>Specify the IP address of an optional alternate DNS server.</td>
</tr>
<tr>
<td>Alternate DNS Server 2</td>
<td>Specify the IP address of an optional alternate DNS server.</td>
</tr>
</tbody>
</table>

**Static Hosts**

The Static Hosts page enables you to edit the hosts file for the Standalone Sentry appliance.

**Figure 1. Static Hosts**

![Static Hosts page](image)

**Adding hosts**

You can add an entry to the hosts file on the Standalone Sentry appliance in the Sentry System Manager.

**Procedure**

1. In the Standalone Sentry System Manager go to **Settings > Static Hosts**.
2. Click the **Add** button.
3. Use the following guidelines to complete the displayed fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address for the host you are adding.</td>
</tr>
<tr>
<td>FQDN</td>
<td>The fully-qualified domain name for this host, as in myserver.mycompany.com.</td>
</tr>
<tr>
<td>Alias</td>
<td>The alias for this host. Up to 29 aliases are allowed.</td>
</tr>
</tbody>
</table>

NOTE: No more than 799 characters are allowed for each host entry. Each host entry includes the IP address, FQDN, and the alias.

4. Click **Save**.

**Editing hosts**

To edit an entry in the hosts file on the Sentry appliance, click the IP address for the host displayed in the Static Hosts screen in the Standalone Sentry System Manager in **Settings > Static Hosts**.

**Deleting hosts**

To delete an entry in the hosts file on the Sentry appliance, select the IP address for the host displayed in the Static Hosts screen in the Standalone Sentry System Manager in **Settings > Static Hosts**.

**Procedure**

1. In the Static Hosts screen, select the host to be deleted.
2. Click **Delete**.
Date and Time (NTP)

The Date and Time screen displays any NTP information specified during installation. This is an optional portion of the configuration, but is highly recommended due to the effect of database timestamps on the behavior of the system, as well as on the quality of reporting. Currently, only UTC time display is supported. If you choose to use a local time source, instead, then you can specify the date in this screen.

The following table describes the fields for setting the system date and time.

### Table 1. Date and Time (NTP)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Source</td>
<td>Select NTP if you intend to specify one or more NTP servers. Select Local if you intend to set the system time for the Server.</td>
</tr>
<tr>
<td>If you select NTP</td>
<td></td>
</tr>
<tr>
<td>Primary Server</td>
<td>Specify the IP address or fully-qualified host name for the NTP server to use.</td>
</tr>
<tr>
<td>Secondary Server</td>
<td>Specify the IP address or fully-qualified host name for the first failover NTP server to use.</td>
</tr>
<tr>
<td>Tertiary Server</td>
<td>Specify the IP address or fully-qualified host name for the second failover NTP server to use.</td>
</tr>
</tbody>
</table>
### Table 1. Date and Time (NTP) (Cont.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you select Local</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Enter the current date.</td>
</tr>
<tr>
<td>Time</td>
<td>Enter the current time.</td>
</tr>
</tbody>
</table>

### CLI

The CLI screen displays the command line interface access settings specified during configuration. Use this screen to alter these settings.

For information about using the CLI, see "Command Line Interface" on page 146.

The following table describes the CLI settings.

### Table 1. CLI Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Secret</td>
<td>Click the Change Enable Secret link to specify the password required to access important functions in the CLI.</td>
</tr>
<tr>
<td>Confirm Enable Secret</td>
<td>Re-enter the specified password to confirm. This field displays only if you click the Change Enable Secret link.</td>
</tr>
<tr>
<td>CLI Session Timeout</td>
<td>Specify the duration of inactivity on the SSH connection that should cause the session to time out.</td>
</tr>
<tr>
<td>SSH</td>
<td>Select Enable if you want to allow SSH access to the Administration tool.</td>
</tr>
<tr>
<td>Max SSH Sessions</td>
<td>Specify the maximum number of simultaneous SSH sessions to allow.</td>
</tr>
</tbody>
</table>

### Splunk

You can configure a Splunk entry on Standalone Sentry so that Standalone Sentry periodically sends Sentry health and audit log data to the Splunk Enterprise server set up on your network. Logs are forwarded to the Splunk receiver and to the local log location.

### Overview of the steps for setting up Splunk on Standalone Sentry

Following is an overview of the steps for setting up Splunk on Standalone Sentry:
1. “Enabling the Splunk forwarder service in Standalone Sentry” below.
2. “Adding a Splunk receiver entry in Standalone Sentry” below.
3. “Configuring Standalone Sentry data to export to Splunk” on the next page.
4. “Tasks in Splunk server to set up Standalone Sentry” on the next page

Enabling the Splunk forwarder service in Standalone Sentry

Enable the Splunk forwarder service so that it can push data to the Splunk receiver.

The Splunk forwarder service can also be enabled using CLI.

Procedure
1. In Standalone Sentry System Manager, go to Settings > Services.
2. For Splunk Forwarder, select Enable.
3. Click Apply > OK to save the changes.
   The status for Splunk Forwarder displays as Running.

Next steps

Go to "Adding a Splunk receiver entry in Standalone Sentry" below.

Adding a Splunk receiver entry in Standalone Sentry

You add the Splunk receiver in the Standalone Sentry System Manager in Settings > Splunk.

Procedure
1. In Standalone Sentry System Manager, go to Settings > Splunk.
2. Click Add to open the Add Splunk Receiver window.
3. Configure the fields.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk Receiver</td>
<td>Add the IP address or the hostname of your Splunk Enterprise Server.</td>
</tr>
<tr>
<td>Port</td>
<td>Add the port of your Splunk Enterprise Server.</td>
</tr>
<tr>
<td>Enable SSL</td>
<td>(Optional) Click the check box to enable SSL.</td>
</tr>
</tbody>
</table>

4. Click Apply > OK to save the changes.

Next steps

Go to "Configuring Standalone Sentry data to export to Splunk" on the next page.
Configuring Standalone Sentry data to export to Splunk

Use the Standalone Sentry command line interface (CLI) to configure the data to export to Splunk.

Procedure
1. SSH to Standalone Sentry.
2. In configuration mode, enter sentry audit to enable miauditlogs log data for export.
3. In configuration mode, enter sentry health-monitor to enable mihealth log data for export.
4. Enter end to exit configuration mode.

Next steps

Go to “Tasks in Splunk server to set up Standalone Sentry” below.

Related topics

See "Log representation and format" on page 105 for the representation and the format of the data captured in audit and health logs.

Tasks in Splunk server to set up Standalone Sentry

Do the following on the Splunk server:
1. Ensure that Splunk listener is on the same port as the one configured in the Splunk entry in Standalone Sentry.
2. Enable the miauditlog and mihealth indexes, which are sentry_miaudit and sentry_mihealth respectively.

Syslog

You can send Sentry syslog data to a remote log server you have set up on your network. Logs are then written to both the syslog location and the local log location.

Adding a syslog entry

You add the syslog server in the Standalone Sentry System Manager in Settings > Syslog.

Procedure
1. In Sentry System Manager, go to Settings > Syslog.
2. Click Add.
3. Enter the requested information.
4. Click Apply.
Related topics

See the field descriptions for a Syslog entry in "Field descriptions for a syslog entry" below.

Editing a syslog server entry

Settings > Syslog lists the syslog server you have configured on Sentry. You can edit the syslog server setting you have configured.

Procedure

1. In Sentry System Manager, go to Settings > Syslog.
2. Click on the IP address or hostname of the syslog server you want to edit.
3. Update the settings as needed.
   - You cannot update the server address or hostname.
4. Click Apply to save and apply the changes.

Related topics

See the field descriptions for a Syslog entry in "Field descriptions for a syslog entry" below.

Field descriptions for a syslog entry

The following table describes the settings for syslog.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Enter the IP address or host name for the remote log server.</td>
</tr>
<tr>
<td>Port</td>
<td>The default is port 514. Monitor listens on port 514. If you are using Monitor, use the default port 514 for both TCP and UDP.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select UDP or TCP. Select UDP or TCP, depending on whether your syslog server is set up to receive UDP or TCP data.</td>
</tr>
</tbody>
</table>
**TABLE 1. SYSLOG FIELDS DESCRIPTION (CONT.)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Type</td>
<td>Select the appropriate facility type to select the logs to report to syslog server. <strong>General</strong>: Select to send mi.log and miservicewatch.log data. The mi.log file contains sentry.log and mics.log data. The miservicewatch.log contains data from <strong>Troubleshoot &gt; Service Diagnosis</strong> in the Sentry System Manager. <strong>Audit</strong>: Select to send audit logs. <strong>Health Monitor</strong>: Select to send health monitoring logs.</td>
</tr>
<tr>
<td>Log Level</td>
<td>Select a log level from the drop down list. The log level is listed based on the priority and severity of the log message. <strong>Emergency</strong>, <strong>Alert</strong>, <strong>Critical</strong>, <strong>Error</strong>, <strong>Warning</strong>, <strong>Notice</strong>, <strong>Info</strong>, <strong>Debug</strong>. Emergency has the highest priority and Debug the lowest priority. All log messages at that log level and higher priority are included in the log file. For Facility type <strong>Audit</strong> and <strong>Health Monitor</strong>, <strong>Info</strong> is the only log level available.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Select <strong>Enable</strong> from the dropdown list to apply these settings to your current configuration. Select <strong>Disable</strong> to suspend use of the configured log server.</td>
</tr>
</tbody>
</table>

**Adding Monitor as a syslog server**

Monitor allows IT and system administrators to monitor the health of all their mission-critical UEM components and services. Monitor organizes and displays monitoring data pushed from Sentry, providing you a comprehensive view of system status and alerts.

**Before you begin**

- You must have set up Monitor. For information on how to set up Monitor, see the *Monitor Configuration Guide*. |
Procedure:

1. In Sentry System Manager, go to **Settings > Syslog**.
2. Click **Add**.
3. Provide values for the Add Syslog dialog fields:
   a. **Server**: Enter the IP address of Monitor.
   b. **Port**: Use the default port 514.
   c. **Protocol**: Select the desired protocol.
   d. **Facility Type**: Select General.
      Only General is supported.
   e. **Log Level**: Select the desired log level.
   f. **Admin State**: Select **Enable**.
4. Click **Apply**.

**SNMP**

Simple Network Management Protocol (SNMP) is a protocol used for network management for collecting information about network entities, such as servers and devices, on an Internet Protocol (IP) network. Various third-party SNMP systems are available that provide SNMP-based management and tools.

Sentry provides the following SNMP capabilities:

- Link up and down traps
  Sentry sends these two SNMP traps (events) to a specified SNMP trap receiver using the SNMP v2c protocol.

- An SNMP server can request information from Sentry related to these MIBs:
  - The HOST-RESOURCES_MIB
  - disk I/O (UCD-DISKIO-MIB)

- Support for SNMP v2c and v3 protocols to pull MIB information from Sentry to the SNMP server.
  It is recommended to use v3 protocol if you transmit information across unsecured links.

Use the SNMP screen to manage SNMP trap receivers.

**Configuring SNMP on Sentry**

The following provides the general workflow to configure SNMP:
1. "Configuring the SNMP trap receiver server" below to which Sentry sends SNMP traps.

2. "Enabling the SNMP service with the v3 protocol" on the next page from whom Sentry accepts requests.

3. "Enabling the SNMP service with the v2c protocol" on page 92 between Sentry and your SNMP server.

**Configuring the SNMP trap receiver server**

Configure the server to which Sentry sends SNMP traps. This server can also get MIB information from Sentry.

**Procedure**

1. Log into Sentry.

2. Go to **Settings > SNMP** to open the SNMP details pane.

3. Click **Add** to open the **Add SNMP Trap Receiver** window.

4. Edit the fields, as necessary.
   Refer to the "SNMP" on the previous page table for details.

5. Click **Apply > OK** to save the changes.

**Add SNMP trap receiver field description**

The following table summarizes fields and descriptions in the **Add SNMP Trap Receiver** window:

<table>
<thead>
<tr>
<th><strong>Table 1. Fields and descriptions in the Add SNMP Trap Receiver window</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fields</strong></td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Community</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Admin State</td>
</tr>
</tbody>
</table>
**Editing a trap receiver**

To edit an SNMP trap receiver, navigate to Settings > SNMP in the Standalone Sentry System Manager.

**Procedure**

1. In the Standalone Sentry System Manager, navigate to Settings > SNMP.
2. In the SNMP screen, select the link for the trap receiver you want to edit.
3. Make your changes.
4. Click Save.

**Deleting SNMP trap receiver servers**

To delete one or more SNMP trap receiver servers, navigate to Settings > SNMP in the Standalone Sentry System Manager.

**Procedure**

1. In the Standalone Sentry System Manager, navigate to Settings > SNMP to open the SNMP details pane.
2. Select one or more of the servers you want to delete. Click the box next to Server to select all servers in the list.
3. Click Delete > Yes.

**Enabling the SNMP service with the v3 protocol**

Set up the SNMP v3 user from whom Standalone Sentry accepts requests. In addition, you can enable or disable sending traps to any configured SNMP trap receiver.

**Procedure**

1. Log into Standalone Sentry System Manager.
2. Go to Settings > SNMP to open the SNMP details pane.
3. In the SNMP Control section, select Enable for SNMP Service to enable the SNMP service on Standalone Sentry.
4. Go to the **Protocol** option and verify that **v3** is selected. The v3 option is selected, by default.

**FIGURE 1. SNMP SERVICE**

5. Click **Add** to open the **Add SNMP v3 User** window.

6. Enter the SNMP v3 user fields, as necessary.

7. Click **Save** to add this user to the **SNMP v3 Users** table.

8. Go to **Link Up/Down Trap**.

9. Select **Enable**.
   Select **Disable** to stop Sentry from sending SNMP traps to any SNMP trap receiver.

10. Click **Apply > OK** to save the changes.
Related topics
Refer to the "SNMP" on page 87 for details.

SNMP v3 User field description

The following table describes the SNMP v3 user fields.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter the username without any spaces (example: miuser).</td>
</tr>
<tr>
<td>Security Level</td>
<td>Select a security level for authentication. The options are:</td>
</tr>
<tr>
<td></td>
<td>• noAuthNoPriv: Without Authentication or Privacy.</td>
</tr>
<tr>
<td></td>
<td>• authNoPriv: With Authentication and without Privacy</td>
</tr>
<tr>
<td></td>
<td>• authPriv: With Authentication and with Privacy</td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>Select an authentication protocol. This can be selected only if the Security Level is selected as authNoPriv or authPriv.</td>
</tr>
<tr>
<td>Auth Password</td>
<td>Enter a password for authentication. The password must contain at least characters.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>Select a privacy protocol. This can be selected only if Security Level is selected as authPriv.</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>Enter a privacy password with minimum of 8 characters.</td>
</tr>
</tbody>
</table>

Deleting SNMP v3 users

The following describes how to delete one or more SNMP v3 users.

Procedure
1. Log into Sentry.
2. Go to Settings > SNMP to open the SNMP details pane.
3. Go to the SNMP Control group.
4. Select one or more of the users you want to delete.
   Click the box next to User Name to select all users in the list.
5. Click Delete > Yes.
Enabling the SNMP service with the v2c protocol

Set up the SNMP v2c communication between Sentry and your SNMP server. You also enable or disable sending traps to any configured SNMP trap receiver.

Procedure

1. Log into Sentry.
2. Go to Settings > SNMP to open the SNMP details pane.
3. Go to the SNMP Control section > SNMP Service.
4. Select Enable to enable the SNMP service on Standalone Sentry.
5. Go to the Protocol option and select v2c.
6. Change the value of Read Only Community if necessary.
   The standard SNMP community string name is public. This is the community string that the SNMP server uses to pull MIB information from Sentry.
7. Go to the Link Up/Down Trap option and select Enable.
   Select Disable to stop Sentry from sending SNMP traps to any SNMP trap receiver.
8. Click Apply > OK to save the changes.

Editing the Read Only Community string

The community string is available for v2 protocol. The default community string for the SNMP is set to public. To change this string, navigate to Settings > SNMP in the Standalone Sentry System Manager.

Procedure

1. In the Standalone Sentry System Manager, navigate to Settings > SNMP.
2. Edit the default string.
3. Click Apply.

Email Settings

Use the Email Settings page to configure the SMTP server. This configuration is required for Sentry monitoring alert notifications by email.
Configuring the SMTP server information for Standalone Sentry notifications

Configure the SMTP server information required for Sentry alert notifications.

Procedure
1. In the Sentry System Manager, go to **Settings**.
2. Click **Email Settings** in the left navigation pane.
3. Enter the requested information.
4. Click **Test**.
5. Enter an email address and body for the test email.
6. Click **OK**.
7. Confirm that the email arrives as expected.
8. Click **Save**.

Related topics

For a description of the fields for configuring SMTP, see "Field descriptions for SMTP settings" below.

Field descriptions for SMTP settings

The following table describes the fields for configuring SMTP settings.
TABLE 1. FIELD DESCRIPTIONS FOR SMTP SETTINGS

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Email</td>
<td>Specify the email address to use in the From field for all administrative email notifications.</td>
</tr>
<tr>
<td>SMTP Server</td>
<td>Specify the IP address or fully-qualified host name for the SMTP server the Ivanti Server will use.</td>
</tr>
<tr>
<td>SMTP Server Port</td>
<td>Specify the port configured for the SMTP server.</td>
</tr>
<tr>
<td>Protocol</td>
<td>If the SMTP server you are configuring is a secured server, that is, it uses the SMTPS protocol, then select the SMTPS button. Otherwise, leave SMTP selected.</td>
</tr>
<tr>
<td>Authentication Required</td>
<td>Specify whether this SMTP server requires authentication. In most cases, this field will be set to Yes.</td>
</tr>
<tr>
<td>User Name</td>
<td>If you select Yes for Authentication Required, then this field displays. Enter the user name required for SMTP authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>If you select Yes for Authentication Required, then this field displays. Enter the password required for SMTP authentication.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>If you select Yes for Authentication Required, then this field displays. Confirm the password required for SMTP authentication.</td>
</tr>
</tbody>
</table>

Login

Use the Login page to add disclaimers. This banner appears on the log in page for Sentry.

The banner does not appear on the Sentry log in page until the disclaimer is updated in the Sentry Settings.
Procedure
1. In the Sentry System Manager, go to **Settings**.
2. Click **Login** in the left navigation pane.
3. Enter the text to display in the Login Banner.
4. Click **Apply**.
5. Click **Yes** to confirm the configuration.

**Timeout**

Use the **Timeout** page to configure the idle session timeout for Sentry System Manager. You can set the timeout for up to 90 minutes.

> Idle Session Timeout will be applicable for the next sessions only.

Procedure
1. In the Sentry System Manager, go to **Settings**.
2. Click **Timeout** in the left navigation pane.
3. Select the Idle Session Timeout for the System Manager portal.
4. Click **Apply**.

5. Click **Ok**.

**Services**

Use the **Services** screen to enable or disable the Sentry service. Select **Enable** or **Disable**, then click **Apply**. The status displays to the right of the setting. **Running** indicates that the Sentry service is enabled. **Not Running** indicates that the Sentry service is disabled.
Figure 1. Enable or disable Sentry service

Sentry

Use the Settings > Services > Sentry screen to change the default setting for whether new devices are allowed or not allowed to access the ActiveSync server or backend resource when UEM is inaccessible.

Figure 1. New device access when UEM is unreachable
New device access

Use the **New device access when EMM server is unreachable** setting to allow or block new devices or devices not in the Standalone Sentry cache, access to the ActiveSync server or backend resource if UEM is not reachable.

By default Standalone Sentry allows new devices access to the server if the UEM is not reachable.

Changing the **New device access when UEM server is unreachable** setting does not restart Standalone Sentry.

To block new devices from accessing the server when UEM is unreachable, select **Block** from the drop down list and click **Apply**.

Incoming SSL configuration

For Cloud, cipher suites and protocols configuration is done in the Sentry profile on Cloud.

Outgoing SSL configuration

For Cloud, cipher suites and protocols configuration is done in the Sentry profile on Cloud.

The **Outgoing SSL Configuration** page Allows administrators the flexibility to configure Standalone Sentry to use cipher suites and protocols to match the security and system needs of your enterprise.

UEM SSL Configuration

Use the **UEM SSL Configuration** page to configure the client role parameters for communication from Sentry to UEM. You can configure ciphers and protocols for outgoing traffic from Sentry to UEM.

- "Enabling Strict TLS" on the next page settings for Standalone Sentry SSL connections to UEM.
- “Enabling Server Name Indication (SNI)” on the next page.
- View the **Available** and **Selected** protocols and cipher suites. See "Cipher Suites and Protocols" on page 100.
- Set up custom protocol and cipher suite configuration. See "Cipher Suites and Protocols" on page 100.

The **EMM SSL Configuration page** allows the administrator the flexibility to configure Standalone Sentry to use cipher suites and protocols to match the security and system needs of your enterprise.
Enabling Strict TLS

You can enable strict TLS for outgoing traffic from Standalone Sentry to UEM. Strict TLS is not enabled by default for the UEM server. However, it is enabled for Cloud. When you enable strict TLS, the Java Trust Store is enabled by default. You can also use the custom trust store option to upload additional certificates that Standalone Sentry must use.

Procedure

1. In the Standalone Sentry System Manager, go to Settings > Services > Sentry > EMM SSL Configuration.
2. In the Strict TLS Settings section, check Enable Strict TLS.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Default Java Trust Store</td>
<td>Selected by default if strict TLS is enabled. Certificates and Certificates Authorities in the Java Trust Store are used to trust the SSL connection to UEM.</td>
</tr>
<tr>
<td>Allow and Log untrusted servers</td>
<td>Select to allow Standalone Sentry to connect to UEM that does not use a trusted certificate in Java or custom trust store.</td>
</tr>
<tr>
<td>Enable Custom Trust Store</td>
<td>Select to upload certificates to the Standalone Sentry trust store. Standalone Sentry uses the certificates in the custom store to trust UEM. Generally used if UEM uses self-signed certificates.</td>
</tr>
</tbody>
</table>

3. Click Apply.
4. Click Yes.

The new TLS settings are applied and Standalone Sentry restarts. It may take up to one minute for Standalone Sentry to restart. Traffic is disrupted till Standalone is up and running again.
5. Click OK.

Enabling Server Name Indication (SNI)

Server Name Indication (SNI) is an extension to TLS. SNI allows multiple hostnames to be served over HTTPS from one IP address. By default, SNI is disabled on Standalone Sentry for outgoing connections for the UEM server. However, SNI is enabled (read-only) for Cloud UEM server. SNI allows a load balancer to direct incoming traffic to the correct UEM server based on the hostname provided by the client, in this case, Standalone Sentry. Some UEM servers may require that SNI is enabled in the client. Your Active Directory Federation Services (ADFS) may require SNI for all client communications.
If SNI is enabled for EMM SSL connections, in some cases health check may fail if the backend server does not also support SNI. The workaround is to disable health check for the impacted server.

Procedure

1. In Standalone Sentry System Manager, go to Settings > Services > Sentry > EMM SSL Configuration.
2. Click Enable SNI.
3. Click Apply.

Cipher Suites and Protocols

Standalone Sentry includes a set of cipher suites and protocols. A default set of cipher suites and protocols is available in the Selected column. You can customize the Selected list of ciphers and protocols to match the security and system needs for your enterprise.

The available and default set of cipher suites and protocols may be updated in a release. Some cipher suites and protocols may be added, while others may be removed. Cipher suites and protocols may be removed if the platform no longer supports these cipher suites and protocols.

If you are set up to use the default cipher suites and protocols, these will be updated to the latest defaults when you upgrade to a new version of Standalone Sentry. If you are set up to use a custom list of Selected cipher suites and protocols, the custom list is preserved when you upgrade your Standalone Sentry. However, any cipher suites or protocols that were removed will also be removed from the Selected and Available columns. New cipher suites and protocols will be added to the Available column.

WARNING: Making changes to the selected list of cipher suites may impact the performance and security of traffic through Standalone Sentry. Therefore, before making any changes to the Selected cipher suites, Ivanti recommends that you understand both the performance and security impact of the changes.

Note The Following:

- SSLv2Hello is a pseudo-protocol that allows Java to initiate the handshake with an SSLv2 'hello message.' This does not cause the use of the SSLv2 protocol, which is not supported by Java. SSLv2Hello requires that TLSv1 protocol is also selected.

SSLv2Hello is required by some load balancers and SSL off loaders for proper functioning. If your environment does not need it, it is recommended to remove this from the protocol list for improved security.

Procedure

1. In Standalone Sentry System Manager, go to Settings > Services > Sentry > EMM SSL Configuration. Ciphers and protocols are configured in the Sentry to Backend Ciphers, SNI, and Protocols Configuration section.
The **Use Default Cipher Suites and Protocols (recommended)** option is selected by default.

2. Select **Use Custom Configuration**.
3. Click **Proceed** to continue.
4. Select the protocols and cipher suites to move from the Available to Selected column or vice-versa as necessary.
   The default cipher suites and protocols are colored blue.
5. Click **Apply** to save the changes.

---

When Use Default Cipher Suites and Protocols (recommended) is selected, the cipher suites and protocols can be moved between the Available and Selected columns. However, the configuration is not changed. You must also select the Use Custom Configuration option to make changes to the default configuration.

---

**Switching back to default configuration**

You can revert your settings to default configuration if you do not wish to use the custom configuration.

**Procedure**

1. In Standalone Sentry System Manager, go to **Settings > Services > Sentry > EMM SSL Configuration**.
2. In the **Sentry to EMM Ciphers, SNI, and Protocols Configuration** section, select **Use Default Cipher Suites and Protocols (recommended)**.
3. Click **Apply** to save the changes.
   The cipher suites and protocols are reset to the default settings.
   Clicking on **Reset to Default** resets the Available and Selected columns to default settings. However, the default settings will not be applied. To apply the default settings, you must select **Use Default Cipher Suites and Protocols (recommended)**, and then click **Apply**.

**Access SSL Configuration**

Use the Access SSL Configuration page to configure the client role parameters for communication from Sentry to Access. You can configure ciphers and protocols for outgoing traffic from Sentry to Access.

- "Managing Strict TLS" on the next page settings for Standalone Sentry SSL connections to Access.
- "Server Name Indication (SNI)" on page 103.
- View the Available and Selected protocols and cipher suites. See "Cipher suites and protocols" on page 103.
- Set up custom protocol and cipher suite configuration. See "Customizing cipher suites and protocols" on page 104.
The **Access SSL Configuration page** allows the administrator the flexibility to configure Standalone Sentry to use cipher suites and protocols to match the security and system needs of your enterprise.

### Managing Strict TLS

You can enable strict TLS for outgoing traffic from Standalone Sentry to Access. Strict TLS is enabled by default. With strict TLS enabled, the Java Trust Store is enabled by default. You can also use the custom trust store option to upload additional certificates that Standalone Sentry must use.

#### Procedure

1. In the Standalone Sentry System Manager, go to **Settings > Services > Sentry > Access SSL Configuration**.
2. In the **Strict TLS Settings** section, select or deselect **Enable Strict TLS** to enable or disable Strict TLS appropriately. Additional options are now available.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Default Java Trust Store</td>
<td>Selected by default if strict TLS is enabled. Certificates and Certificates Authorities in the Java Trust Store are used to trust the SSL connection to UEM.</td>
</tr>
<tr>
<td>Allow and Log untrusted servers</td>
<td>Select to allow Standalone Sentry to connect to UEM that does not use a trusted certificate in Java or custom trust store.</td>
</tr>
<tr>
<td>Enable Custom Trust Store</td>
<td>Select to upload certificates to the Standalone Sentry trust store. Standalone Sentry uses the certificates in the custom store to trust UEM. Generally used if UEM uses self-signed certificates.</td>
</tr>
</tbody>
</table>

3. Click **Apply**.
4. Click **Yes**.
   The new TLS settings are applied and Standalone Sentry restarts. It may take up to one minute for Standalone Sentry to restart. Traffic is disrupted till Standalone is up and running again.
5. Click **OK**.
Server Name Indication (SNI)

Server Name Indication (SNI) is an extension to TLS. SNI allows multiple hostnames to be served over HTTPS from one IP address. By default, SNI is enabled on Standalone Sentry for outgoing connections. SNI allows a load balancer to direct incoming traffic to the correct Access server based on the hostname provided by the client, in this case, Standalone Sentry. Access servers require that SNI is enabled in the client. Your Active Directory Federation Services (ADFS) requires SNI for all client communications.

If SNI is enabled for Access SSL connections, in some cases health check may fail if the Access server does not also support SNI. The workaround is to disable health check for the impacted server.

Cipher suites and protocols

Standalone Sentry includes a set of cipher suites and protocols. A default set of cipher suites and protocols is available in the Selected column. You can customize the Selected list of ciphers and protocols to match the security and system needs for your enterprise.

The available and default set of cipher suites and protocols might be updated in a release. Some cipher suites and protocols might be added, while others may be removed. Cipher suites and protocols might be removed if the platform no longer supports these cipher suites and protocols.

If you are set up to use the default cipher suites and protocols, these are updated to the latest defaults when you upgrade to a new version of Standalone Sentry. If you are set up to use a custom list of Selected cipher suites and protocols, the custom list is preserved when you upgrade your Standalone Sentry. However, any cipher suites or protocols that were removed are also removed from the Selected and Available columns. New cipher suites and protocols are added to the Available column.

WARNING: Making changes to the selected list of cipher suites may impact the performance and security of traffic through Standalone Sentry. Therefore, before making any changes to the Selected cipher suites, Ivanti recommends that you understand both the performance and security impact of the changes.

Note The Following:

- SSLv2Hello is a pseudo-protocol that allows Java to initiate the handshake with an SSLv2 ‘hello message.’ This does not cause the use of the SSLv2 protocol, which is not supported by Java. SSLv2Hello requires that r TLSv1 protocol is also selected.

SSLv2Hello is required by some load balancers and SSL off loaders for proper functioning. If your environment does not need it, it is recommended to remove this from the protocol list for improved security.
Customizing cipher suites and protocols

You can customize the cipher suites and protocols configuration.

**Procedure**

1. In Standalone Sentry System Manager, go to **Settings > Services > Sentry > Access SSL Configuration**. Ciphers and protocols are configured in the **Sentry to CMS Ciphers, SNI, and Protocols Configuration** section.
   The **Use Default Cipher Suites and Protocols (recommended)** option is selected by default.
2. Select **Use Custom Configuration**.
3. Click **Proceed** to continue.
4. Select the protocols and cipher suites to move from the **Available** to **Selected** column or vice-versa as necessary.
   The default cipher suites and protocols are colored blue.
5. Click **Apply** to save the changes.

When **Use Default Cipher Suites and Protocols (recommended)** is selected, the cipher suites and protocols can be moved between the Available and Selected columns. However, the configuration is not changed. You must also select the **Use Custom Configuration** option to make changes to the default configuration.

Switching back to default configuration

You can revert your settings to default configuration if you do not wish to use the custom configuration.

**Procedure**

1. In Standalone Sentry System Manager, go to **Settings > Services > Sentry > Access SSL Configuration**.
2. In the **Sentry to CMS Ciphers, SNI, and Protocols Configuration** section, select **Use Default Cipher Suites and Protocols (recommended)**.
3. Click **Apply** to save the changes.
   The cipher suites and protocols are reset to the default settings.

Clicking **Reset to Default** resets the **Available** and **Selected** columns to default settings. However, the default settings are not applied. To apply the default settings, you must select **Use Default Cipher Suites and Protocols (recommended)**, and then click **Apply**.

**Outbound HTTP Proxy**

Use the Outbound HTTP Proxy page to configure the proxy parameters for communication from Sentry to Cloud or Access.
Configuring Outbound HTTP Proxy

The Outbound HTTP Proxy page allows the administrator the flexibility to configure Standalone Sentry with outbound HTTP proxy server settings. The traffic from Sentry passes through the proxy to Cloud or Access. Sentry will use the User Name and Password for authentication if requested by the proxy.

Procedure

1. In Standalone Sentry System Manager, go to Settings > Services > Sentry > Outbound HTTP Proxy.
2. Select Cloud to configure the outbound proxy server settings for Cloud.
   a. Enter the Proxy Host.
   b. Enter the Proxy Port.
   c. Enter the User Name.
   d. Enter the Password.
3. Select Access to configure the outbound proxy server settings for Access.
   a. Enter the Proxy Host.
   b. Enter the Proxy Port.
   c. Enter the User Name.
   d. Enter the Password.
4. Click Apply.

Log representation and format

The following provide the representation and format of the data captured in audit and health logs:

- "Audit log representation and format" below
- "Health log representation and format" on page 111

Audit log representation and format

An audit entry is created for each request from a device. A corresponding response entry is created for each request. The audit logs are in JSON format.

The following provide the format for audit log entries:

- "Audit log entry for a request" on the next page
- "Audit log entry for a response" on the next page
- "Audit log entry for IP VPN response to tunnel establishment request" on page 107
- "Audit log entry for IP VPN internal connection" on page 108
Audit log entry for a request

The following provides a description of the fields in the audit log entry for a request.

**TABLE 1. FIELD DESCRIPTIONS FOR A REQUEST IN AUDIT LOG**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publishTime</td>
<td>Actual time of log capture. Logging time might vary based on async strategies.</td>
</tr>
<tr>
<td>entryID</td>
<td>Unique for every audit entry. GUID.</td>
</tr>
<tr>
<td>useCaseID</td>
<td>ID of use-case to which this entry belongs to. This ID is used for relating Request/Response.</td>
</tr>
<tr>
<td>entryType</td>
<td>REQUEST.</td>
</tr>
<tr>
<td>userId</td>
<td>EMM User ID.</td>
</tr>
<tr>
<td>deviceID</td>
<td>Device identification.</td>
</tr>
<tr>
<td>deviceType</td>
<td>Type of device - iPhone, iPad etc.</td>
</tr>
<tr>
<td>serviceType</td>
<td>ActiveSync, CIFS, Access, APP_TUNNEL, TCP_TUNNEL, IP_TUNNEL.</td>
</tr>
<tr>
<td>serviceName</td>
<td></td>
</tr>
<tr>
<td>clientHost</td>
<td></td>
</tr>
<tr>
<td>clientPort</td>
<td></td>
</tr>
<tr>
<td>requestUrl</td>
<td>URL used by device.</td>
</tr>
<tr>
<td>httpMethod</td>
<td>HTTP method used for this request.</td>
</tr>
<tr>
<td>applicationId</td>
<td></td>
</tr>
<tr>
<td>forwardedFor</td>
<td>If proxy is forwarding request, this will have actual client host identifier.</td>
</tr>
<tr>
<td>contextHeaders</td>
<td></td>
</tr>
<tr>
<td>serverHost</td>
<td>Details of downstream server.</td>
</tr>
<tr>
<td>serverPort</td>
<td></td>
</tr>
<tr>
<td>action</td>
<td>ALLOW</td>
</tr>
</tbody>
</table>

Audit log entry for a response

The following provides a description of the fields in the audit log entry for a response.
### TABLE 2. FIELD DESCRIPTIONS FOR A RESPONSE IN AUDIT LOG

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publishTime</td>
<td>Actual time of log capture. Logging time might vary based on async strategies.</td>
</tr>
<tr>
<td>entryID</td>
<td>Unique for every audit entry. GUID.</td>
</tr>
<tr>
<td>useCaseID</td>
<td>ID of use-case to which this entry belongs to. This ID is used for relating Request/Response.</td>
</tr>
<tr>
<td>entryType</td>
<td>RESPONSE.</td>
</tr>
<tr>
<td>userID</td>
<td>EMM user ID.</td>
</tr>
<tr>
<td>deviceID</td>
<td>Device identification.</td>
</tr>
<tr>
<td>deviceType</td>
<td>Type of device.</td>
</tr>
<tr>
<td>serviceType</td>
<td>ActiveSync, CIFS, Access, APP_TUNNEL, TCP_TUNNEL, IP_TUNNEL.</td>
</tr>
<tr>
<td>serviceName</td>
<td>Name of service.</td>
</tr>
<tr>
<td>clientHost</td>
<td>Immediate client end-point; if coming via proxy, this could be proxy end-point.</td>
</tr>
<tr>
<td>clientPort</td>
<td></td>
</tr>
<tr>
<td>httpStatus</td>
<td>HTTP Response code.</td>
</tr>
<tr>
<td>sentryHost</td>
<td>Standalone Sentry hostname.</td>
</tr>
<tr>
<td>sentryPort</td>
<td>Standalone Sentry port.</td>
</tr>
<tr>
<td>sentryAddress</td>
<td>Standalone Sentry IP address.</td>
</tr>
</tbody>
</table>

**Audit log entry for IP VPN response to tunnel establishment request**

The following provides a description of the fields in the audit log entry for a request to establish an IP VPN tunnel.
### Table 3. Field Descriptions for IP VPN Response to Tunnel Establishment Request in Audit Log

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publishTime</td>
<td>Actual time of log capture. Logging time might vary based on async strategies.</td>
</tr>
<tr>
<td>entryID</td>
<td>Unique for every audit entry. GUID.</td>
</tr>
<tr>
<td>useCaseID</td>
<td>ID of use-case to which this entry belongs to. This ID is used for relating Request/Response.</td>
</tr>
<tr>
<td>entryType</td>
<td>RESPONSE.</td>
</tr>
<tr>
<td>userID</td>
<td>EMM User ID.</td>
</tr>
<tr>
<td>deviceID</td>
<td>Device identification.</td>
</tr>
<tr>
<td>serviceType</td>
<td>IP_TUNNEL.</td>
</tr>
<tr>
<td>clientHost</td>
<td>Immediate client end-point; if coming via proxy, this could be proxy end-point.</td>
</tr>
<tr>
<td>clientPort</td>
<td></td>
</tr>
<tr>
<td>serverPort</td>
<td></td>
</tr>
<tr>
<td>httpStatus</td>
<td>HTTP Response code.</td>
</tr>
</tbody>
</table>

### Audit log entry for IP VPN internal connection

The following provides a description of the fields in the audit log entry for an internal IP VPN tunnel connection.

### Table 4. Field Descriptions for an IP VPN Internal Connection Entry in Audit Logs

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publishTime</td>
<td></td>
</tr>
<tr>
<td>entryID</td>
<td>Unique for every audit entry. GUID.</td>
</tr>
<tr>
<td>useCaseID</td>
<td>ID of use-case to which this entry belongs to. This ID is used for relating Request/Response.</td>
</tr>
<tr>
<td>entryType</td>
<td>IP_VPN_CONN.</td>
</tr>
<tr>
<td>userID</td>
<td></td>
</tr>
</tbody>
</table>
TABLE 4. FIELD DESCRIPTIONS FOR AN IP VPN INTERNAL CONNECTION ENTRY IN AUDIT LOGS (CONT.)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deviceID</td>
<td>IP_TUNNEL.</td>
</tr>
<tr>
<td>clientHost</td>
<td>IP_TUNNEL.</td>
</tr>
<tr>
<td>clientPort</td>
<td>IP_TUNNEL.</td>
</tr>
<tr>
<td>serverHost</td>
<td>IP_TUNNEL.</td>
</tr>
<tr>
<td>serverPort</td>
<td>IP_TUNNEL.</td>
</tr>
<tr>
<td>action</td>
<td>Compliance action like ALLOW, BLOCK, NONE.</td>
</tr>
<tr>
<td>type</td>
<td>Connection type: UDP or TCP.</td>
</tr>
<tr>
<td>sentryHost</td>
<td>Standalone Sentry hostname.</td>
</tr>
<tr>
<td>sentryPort</td>
<td>Standalone Sentry port.</td>
</tr>
<tr>
<td>sentryAddress</td>
<td>Standalone Sentry IP address.</td>
</tr>
</tbody>
</table>

Examples for audit log entries

Following are examples of audit log entries:

- "IPVPN audit log example" below
  - "ActiveSync audit log example" on the next page
  - "HTTP tunnel audit log example" on the next page
  - "TCP tunnel audit log example" on page 111

IPVPN audit log example

2017 Nov  1 04:13:59 eapp123.auto.mobileiron.com SENTRY_AUDIT: INFO {"usecaseId":"U-43fbd6d7-258d-4d55-aa81-cf1ba1533b4","entryType":"RESPONSE","userId":"hdhindsa","deviceId":"22002","serviceType":"IP_TUNNEL","clientHost":"/24.5.120.210","clientPort":44258,"publishTime":"11/01/2017 4:13:59","entryId":"E-6ec1eeda-5d25-4d3b-8107-5101c188830f","serverPort":443,"httpStatus":"200"}
ActiveSync audit log example


2017 Nov 7 21:23:41 app101.auto.mobileiron.com SENTRY_AUDIT: INFO {"usecaseId":"U-ee3608c9-4c88-4b93-8221-bd69c4da900","entryType":"RESPONSE","userId":"testuser0851","deviceId":"HroLBgueAofSIKAcECcHTqd2","deviceType":"MD723LL","serviceName":"ActiveSync","clientHost":"/10.11.80.93","clientPort":61693,"publishTime":"11/07/2017 21:23:39","entryId":"E-49b3b2b2-07c9-4a82-87d3-3f1f45751879","serverHost":"ex2013.auto19.mobileiron.com","serverPort":443,"sentryHost":"10.10.57.239","sentryPort":446,"sentryAddress":"10.25.35.237","httpStatus":"200"}

HTTP tunnel audit log example

2017 Nov 3 23:06:57 eapp074.auto.mobileiron.com SENTRY_AUDIT: INFO {"usecaseId":"U-dd7086fc-9599-4581-a8bc-5a9857ce085b","entryType":"REQUEST","userId":"testuser7331","deviceId":"62b6a6e9-9ca8-4176-85dd-11a7eeace130","deviceType":"iPhone 6","serviceType":"APP_TUNNEL","serviceName":"<ANY>","clientHost":"/10.11.205.8","clientPort":1821,"publishTime":"11/03/2017 23:06:57","entryId":"E-dd7086fc-9599-4581-a8bc5a9857ce085b","serverHost":"wiki.mobileiron.com","serverPort":443,"requestUrl":"https://wiki.mobileiron.com/login.action?os_destination=%2Findex.action&permissionViolation=true","httpMethod":"GET","applicationId":"com.mobileiron.securebrowser","action":"ALLOW"}
TCP tunnel audit log example

Health log representation and format

The following provide the representation and format for Sentry health logs:

- "/var/log/mihealth_export/openPorts.log" below
- "/var/log/mihealth_export/hardware.log" on the next page
- "/var/log/mihealth_export/cpu.log" on the next page
- "/var/log/mihealth_export/vmstat.log" on the next page

/var/log/mihealth_export/openPorts.log

sourcetype: sentry_mihealth_openPorts

<table>
<thead>
<tr>
<th>Proto</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp</td>
<td>9090</td>
</tr>
</tbody>
</table>
... udp 10012

REGEX = (^[^\s]+)\s+(\[[0-9]+\])

FORMAT = Proto: "$1" Port: "$2"

/var/log/mihealth_export/hardware.log

sourcetype: sentry_mihhealth_hardware

<table>
<thead>
<tr>
<th>KEY</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU_TYPE</td>
<td>Intel(R) Xeon(R) CPU E5504 @ 2.00GHz</td>
</tr>
<tr>
<td>CPU_CACHE</td>
<td>4096 KB</td>
</tr>
<tr>
<td>CPU_COUNT</td>
<td>1</td>
</tr>
<tr>
<td>HARD_DRIVES</td>
<td>sda (Virtual disk) 200 GB;</td>
</tr>
<tr>
<td>NIC_TYPE</td>
<td>&lt;notAvailable&gt;</td>
</tr>
<tr>
<td>NIC_COUNT</td>
<td>1</td>
</tr>
<tr>
<td>MEMORY_REAL</td>
<td>2954232 kB</td>
</tr>
<tr>
<td>MEMORY_SWAP</td>
<td>4128764 kB</td>
</tr>
</tbody>
</table>

/var/log/mihealth_export/cpu.log

sourcetype: sentry_mihhealth_cpu

<table>
<thead>
<tr>
<th>CPU</th>
<th>pctUser</th>
<th>pctNice</th>
<th>pctSystem</th>
<th>pctIowait</th>
<th>pctIdle</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>0.00</td>
<td>1.01</td>
<td>1.01</td>
<td>0.00</td>
<td>97.98</td>
</tr>
<tr>
<td>0</td>
<td>0.00</td>
<td>1.01</td>
<td>1.01</td>
<td>0.00</td>
<td>97.98</td>
</tr>
</tbody>
</table>

REGEX = all\s+(\d*\.\d*)\s+(\d*\.\d*)\s+(\d*\.\d*)\s+(\d*\.\d*)\s+(\d*\.\d*)

FORMAT = pctUser::$1 pctNice::$2 pctSystem::$3 pctIowait::$4 pctIdle::$5

/var/log/mihealth_export/vmstat.log

/usr/bin/vmstat

sourcetype: sentry_mihhealth_vmstat

time=2017-09-05 10:24:01, r=5, b=0, swpd=10268, free=80444, buff=109964, cache=845276, si=0, so=0, bi=5, bo=12, in=115, cs=208, us=1, sy=0, id=99, wa=0, st=0
Standalone Sentry Security Settings

The following describe the security settings in the Standalone Sentry System Manager:

Overview of Standalone Sentry security settings .......................................................... 113
Local Users ..................................................................................................................... 113
Password policy .............................................................................................................. 115
Certificate Management ................................................................................................. 116
Access Control Lists ....................................................................................................... 119
Networks and Hosts ......................................................................................................... 122
Network Services ............................................................................................................ 123
Access Control Lists: ACLs ............................................................................................ 125

Overview of Standalone Sentry security settings

The Security tab in System Manager contains links for configuring aspects of Sentry access. The following table summarizes the tasks associated with each link.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Source: Local Users</td>
<td>Create, delete, and manage local users.</td>
</tr>
<tr>
<td>Identity Source: Password Policy</td>
<td>Configure complex passwords for Standalone Sentry.</td>
</tr>
<tr>
<td>Certificate Mgmt</td>
<td>View and manage certificates for Portal HTTPS</td>
</tr>
<tr>
<td>Access Control Lists: Networks &amp; Hosts</td>
<td>Create and manage entries for networks and hosts</td>
</tr>
<tr>
<td>Access Control Lists: Network Services</td>
<td>Create and manage entries for network services</td>
</tr>
<tr>
<td>Access Control Lists: ACLs</td>
<td>Compile access control lists</td>
</tr>
</tbody>
</table>

Local Users

All users in the Standalone Sentry System Manager database are local users having the following privileges, which cannot be changed:

• Command Line Interface (CLI)
• System Manager access
Adding local users for System Manager

You can add local users in the Standalone Sentry System Manager.

Procedure

1. Go to Security > Local Users.
2. Click Add. The Add New User window displays.
3. Use the following guidelines to complete the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>Enter the unique identifier to assign to this user.</td>
</tr>
<tr>
<td>First Name</td>
<td>Enter the user’s first name.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the user’s last name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password for the user. For password requirements, see &quot;Password policy&quot; on the next page</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Confirm the password for the user.</td>
</tr>
<tr>
<td>Group</td>
<td>This field is not configurable.</td>
</tr>
<tr>
<td>Email</td>
<td>Enter the user’s email address.</td>
</tr>
<tr>
<td>EDIPI</td>
<td>Enter the unique identifier assigned to this user. This is a mandatory field to configure CAC.</td>
</tr>
</tbody>
</table>

4. Click Apply.
5. Click Save.

Editing local users for System Manager

You can change the information for local users in the Standalone Sentry System Manager.

Procedure

1. Go to Security > Local Users.
2. Select the user ID of the entry to display the information for that user.
3. Make your changes.

NOTE: You cannot change the user ID.
4. Click Apply.
5. Click Save.

Deleting local users for System Manager

You can delete local users in the Standalone Sentry System Manager.
Procedure
1. Go to Security > Local Users.
2. Select the checkbox for the user you want to delete.
3. Click Delete.
NOTE: You cannot delete the user ID you logged in with.
4. Click Save.

Password policy
Password policy lets you configure complex passwords for Standalone Sentry.

Configuring password policy
To configure the settings in the Standalone Sentry System Manager, go to Security > Identity Source.

Before you begin
- Verify that you have added local users for System Manager.

Procedure
2. Select Password Policy.
3. Configure the password policy for local users appropriately.

<table>
<thead>
<tr>
<th>Policy</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Number of Character Classes in Password</td>
<td>1 to 4. Passwords must contain at least one upper case character, one lower case character, and one numeric character by default.</td>
</tr>
<tr>
<td>Lower Case</td>
<td>Enable or Disable</td>
</tr>
<tr>
<td>Upper Case</td>
<td>Enable or Disable</td>
</tr>
<tr>
<td>Numeric</td>
<td>Enable or Disable</td>
</tr>
<tr>
<td>Special Character</td>
<td>Enable or Disable. Password can contain special characters only from this set &quot;!=&quot;([[:<del>;</del>,:]]@#</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>Passwords must have at least 6 characters. The length is set to 8 by default.</td>
</tr>
<tr>
<td>Policy</td>
<td>Values</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Password Length</td>
<td>Password length can extend up to 128 characters. The length is set to 32 by default.</td>
</tr>
<tr>
<td>Number of Failed Attempts</td>
<td>Failed password attempts are limited from 1 to 16. The number of attempts is set to 5 by default.</td>
</tr>
<tr>
<td>Auto-Lock Time</td>
<td>0-3600 seconds. You can set the time for password auto-lock.</td>
</tr>
<tr>
<td>Enforce Passcode History</td>
<td>Enable or Disable.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.
5. Click **Yes** to confirm the change.
6. Click **OK** to save the password policy configuration.

## Certificate Management

Use the Certificate Management feature in the Sentry System Manager in **Security > Certificate Mgmt** to manage the certificate required for browsers to access the Standalone Sentry System Manager.

You can perform the following tasks from the Certificate Management screen:

- Generate a self-signed certificate
- Generate a certificate signing request (CSR) for a certificate authority (CA)
- Upload a certificate.

---

> When you update a certificate, you are prompted to confirm that you want to proceed because the HTTP service needs to be restarted, resulting in service disruption.

---

### Generating a self-signed certificate for the Standalone Sentry portal

If you use a self-signed certificate, a browser that is connecting to the Sentry System Manager is warned that the Sentry certificate is not from a trusted source. Therefore, Ivanti recommends that you use a certificate from a trusted Certificate Authority (CA).

To generate a self-signed certificate, in the Sentry System Manager go to **Security > Certificate Mgmt**.

**Procedure**

1. Click the **Manage Certificate** link for **Portal HTTPS**.
2. For **Certificate Options**, select **Generate Self-Signed Certificate** from the dropdown list.
3. Click the **Generate Self Signed Certificate** button.

**Generating a certificate signing request (CSR)**

To get a certificate from a trusted Certificate Authority (CA), use the **Security > Certificate Mgmt** page to generate a certificate signing request (CSR) to the CA. Once you receive the signed certificate, you can use the same page to upload it to Sentry.

**Procedure**

1. Click the **Manage Certificate** link for **Portal HTTPS**.
2. For **Certificate Options**, select **Generate CSR** from the dropdown list.
3. Use the following guidelines to complete the displayed form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>Enter the server host name.</td>
</tr>
<tr>
<td>E-Mail</td>
<td>Enter the email address of the contact person in your organization who should receive the resulting certificate.</td>
</tr>
<tr>
<td>Company</td>
<td>Enter the name of the company requesting the certificate.</td>
</tr>
<tr>
<td>Department</td>
<td>Enter the department requesting the certificate.</td>
</tr>
<tr>
<td>City</td>
<td>Enter the city in which the company is located.</td>
</tr>
<tr>
<td>State</td>
<td>Enter the state in which the company is located.</td>
</tr>
<tr>
<td>Country</td>
<td>Enter the two-character abbreviation for the country in which the company is located.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Length</td>
<td>Select 2048 or 3072 to specify the length of each key in the pair. Longer keys provide stronger security, but may impact performance.</td>
</tr>
</tbody>
</table>

4. Click **Generate**.
A message similar to the following displays.

**Figure 2. Certificate Request**

5. Copy the content between BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY to another text file.
6. Click **Close**.
7. Submit the file you created in step "Certificate Management" on page 116 to the certifying authority.

### Uploading certificates

To upload the CA certificate from the certifying authority in the Standalone Sentry System Manager go to **Security > Certificate Mgmt.**

**Procedure**

1. Click the **Manage Certificate** link for **Portal HTTPS**.
2. For **Certificate Options**, select **Upload Certificate**.
3. Select the certificates as indicated in the following table:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>File to Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key file</td>
<td>The file created in “Generating a certificate signing request (CSR)” on the previous page.</td>
</tr>
</tbody>
</table>
**Certificate** | **File to Select**
---|---
Server certificate | The CA certificate file you received from the certifying authority.
CA certificate | The generic CA certificate file.

4. Click the **Upload Certificate** button.

**Viewing certificates**

To view a certificate, in the Standalone Sentry System Manager go to **Security > Certificate Mgmt** and click the **View Certificate** link for Portal HTTPS.

**Access Control Lists**

Use the Access Control Lists screen in the Standalone Sentry System Manager in **Security > Access Control Lists** to compile and manage the rules that define inbound and outbound access for network hosts and services.

**FIGURE 1. ACCESS CONTROL LISTS**

Each access control list (ACL) consists of one or more access control entries (ACEs). Configuring ACLs requires the following tasks:

1. Configure entries for each network and host requiring an ACL.
2. Configure entries for any network services requiring an ACL.
3. Create an ACL.

**Adding an ACL**

To configure an access control list in the Standalone Sentry System Manager, go to **Security > Access Control Lists**.
Procedure
1. In the Standalone Sentry System Manager, go to Security > Access Control Lists.
2. Click Add.
3. In the Name field, enter a name to identify the ACL.
4. In the Description field, enter text to clarify the purpose of the ACL.
5. Click Save.
   The lower portion of the screen is now enabled.

**Figure 2. Add ACL**

6. Click Add to add an access control entry (ACE) to the ACL.
   Each ACE consists of a combination of the network hosts and services you configured for use in ACLs.
7. Use the following guidelines to complete the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Network</td>
<td>Select the network from which access will originate. This list is populated with the networks and hosts you created for use with ACLs. See &quot;Networks and Hosts on page 122&quot; on &quot;Networks and Hosts&quot; on page 122.</td>
</tr>
<tr>
<td>Destination Network</td>
<td>Select the network being accessed. This list is populated with the networks and hosts you created for use with ACLs. See &quot;Networks and Hosts on page 122&quot; on &quot;Networks and Hosts&quot; on page 122.</td>
</tr>
<tr>
<td>Service</td>
<td>Select the network service to which this entry permits or denies access. This list is populated with the services you created for use with ACLs. See &quot;Network Services&quot; on page 123 on &quot;Network Services&quot; on page 123.</td>
</tr>
<tr>
<td>Action</td>
<td>Select Permit or Deny from the dropdown list.</td>
</tr>
</tbody>
</table>

Close
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connections Per Minute</td>
<td>Enter the number of connections to allow per minute.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter text to describe the purpose of this entry.</td>
</tr>
</tbody>
</table>

8. Click **Save**.

**Editing an ACL**

To edit an access control list in the Standalone Sentry System Manager, go to **Security > Access Control Lists**.

**Procedure**

1. In the Standalone Sentry System Manager, go to **Security > Access Control Lists**.
2. Click the name in the ACLs list.

3. To delete an ACE, click its checkbox and click **Delete**.
4. To add an ACE, click **Add**.
5. To insert an ACE, select the ACE above which you want to insert a new ACE and click Insert.
6. Click **Save**.

**Copying an ACL**

To create a copy of an existing ACL in Standalone Sentry, go to **Security > Access Control Lists**.

**Procedure**

1. In the Standalone Sentry System Manager, go to **Security > Access Control Lists**.
2. Select the ACL to be copied.
3. Click the **Copy** button.
4. Enter a name for the new ACL.
5. Click OK.

Deleting an ACL

To delete an existing ACL in Standalone Sentry, go to Security > Access Control Lists.

Procedure
1. In the Standalone Sentry System Manager, go to Security > Access Control Lists.
2. Select the ACL to be deleted.
3. Click Delete.

Networks and Hosts

Use the Networks and Hosts screen to manage the servers and subnets you will use to compile Access Control Lists (ACLs).

Figure 1. Network and Hosts

Adding a host or subnet for compiling ACLs

To add a host or subnet for compiling ACLs in the Standalone Sentry System Manager, go to Security > Access Control Lists > Network & Hosts.

Procedure
1. Click Add.
2. Use the following guidelines for completing the displayed form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to use to identify this host or network.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter additional text to provide supporting information about this host or network.</td>
</tr>
<tr>
<td>Type</td>
<td>Select Subnet or Host from the dropdown menu.</td>
</tr>
<tr>
<td>Network/Host</td>
<td>Enter the IP address for this network or host.</td>
</tr>
</tbody>
</table>

3. Click Save.
   This host or network will now be available for ACLs configured in the ACLs screen.

**Network Services**

Use the Network Services screen to manage available services. Ivanti prepopulates this screen with common services.
Adding a network service

To add a network service for compiling ACLs in the Standalone Sentry System Manager, go to **Security > Access Control Lists > Network Services**.

**Procedure**

1. Click **Add**.

**Figure 2. Add network service**

2. Use the following guidelines to complete the form:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name to use to identify this service.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter additional text to provide supporting information about this service.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>Select TCP, UDP, or IP from the dropdown menu.</td>
</tr>
<tr>
<td>Source Port</td>
<td>Enter the number of the source port for this service. Enter 0 to allow any source port.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Enter the number of the destination port for this service. Enter 0 to allow any destination port.</td>
</tr>
</tbody>
</table>

3. Click **Save**.

**Access Control Lists: ACLs**

See “‘Access Control Lists” on page 119’” on "Access Control Lists” on page 119.”
Standalone Sentry Maintenance Settings

The following describe the maintenance settings in the Standalone Sentry System Manager:

Overview of Sentry maintenance features .................................................. 126
Updating Standalone Sentry software ...................................................... 126
Exporting the configuration .................................................................. 128
Importing a configuration ...................................................................... 129
Clearing the configuration ...................................................................... 129
Rebooting ............................................................................................... 130

Overview of Sentry maintenance features

The Maintenance tab in the Standalone Sentry System Manager provides basic maintenance features for Standalone Sentry appliance. The following table summarizes these features.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Updates</td>
<td>Upgrade Standalone Sentry software.</td>
</tr>
<tr>
<td>Export Configuration</td>
<td>Save the system configuration file.</td>
</tr>
<tr>
<td>Import Configuration</td>
<td>Import a saved system configuration file.</td>
</tr>
<tr>
<td>Clear Configuration</td>
<td>Clear the current system settings.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Restart the Standalone Sentry.</td>
</tr>
</tbody>
</table>

Updating Standalone Sentry software

If you are upgrading using a URL and not using the Default setting, use the CLI upgrade method. See "Upgrading using CLI" on page 180.

Before you begin

See the Standalone Sentry Release and Upgrade Notes for release specific information.

Procedure

1. In Sentry System Manager, go to Maintenance > Software Updates.
2. Software Version: Check the Standalone Sentry version.
3. Set up the Software Repository Configuration.
   a. Enter the credentials assigned by Support.
   b. For URL, Default is selected.
   c. Click Apply.
   d. Click OK to dismiss the success popup.

4. (Optional) If you are using a proxy server to support.mobileiron.com, set up Software Repository Proxy Configuration.
   a. Hostname/IP: Enter the proxy server hostname or IP address.
   b. Port: Enter the port number on the proxy server for Sentry.
   c. (optional) If needed, enter the credentials for the proxy server.
   d. Click Apply.
   e. Click OK to dismiss the success popup.

5. Click Check Updates.
The available updates are listed.

6. Click Download Now if you want to download the update now and complete the installation at a later time.

7. Refresh the screen and click Check Updates.
   After the download is complete, the status for the update changes to Downloaded.

8. Click Stage for Install when you are ready to install.
   If you had already downloaded the selected update, the system stages the update for installation.
   If you did not previously download the selected update, it is downloaded and staged for installation.
   After the software update has been staged for installation, the status for the update changes to Reboot to Install. You can now install the update by rebooting the system. If the status of an update is not Reboot to Install, rebooting the system will not install the update.

9. Click Reboot in the left navigation pane to install the software update.

Verifying that the upgrade is complete

The following allow you to verify that the Standalone Sentry update is complete.
Procedure

1. In Standalone Sentry System Manager, go to Maintenance > Software Updates. Confirm that the version displayed is the current version.
2. In Standalone Sentry System Manager, go to Troubleshooting > Service Diagnosis. Confirm that status for the services listed shows Success.
3. Enroll a test device and validate email flow by sending and receiving email on the device.

Software update status

The following tables describes the status shown for each software upgrade:

TABLE 1. SOFTWARE UPGRADE STATUS

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Downloaded</td>
<td>The update is not yet downloaded. Next Step: Click Download Now or Stage for Install to download the update.</td>
</tr>
<tr>
<td>Download in progress</td>
<td>The download is in progress. Refresh the browser to update the status.</td>
</tr>
<tr>
<td>Downloaded</td>
<td>The software update has been downloaded. Next Step: Click Stage for Install to stage the update for installation. The software update must be staged before installing.</td>
</tr>
<tr>
<td>Reboot to install</td>
<td>The software update was successfully downloaded and update is staged for the installation. Next Step: Click Reboot in the left navigation pane to install the software update.</td>
</tr>
</tbody>
</table>

Exporting the configuration

To back up the system configuration, you can export the Standalone Sentry configuration settings to XML format.

Procedure

1. Select Export Configuration.
2. Click **Export**.

**Importing a configuration**

You can import a Standalone Sentry configuration from a local XML file or FTP site.

**Procedure**

1. In the Standalone Sentry system manager, go to **Maintenance**.
2. Select **Import Configuration**.

3. Click **Browse** to select an import file.
4. Click **Import**.

**Clearing the configuration**

**Clear Configuration** allows you to clear unsaved configuration settings and return to the default configuration.

**Procedure**

1. In the Standalone Sentry system manager, go to **Maintenance**.
2. Click **Clear Configuration**.

**FIGURE 1. CLEAR CONFIGURATION**

3. Click the **Clear Configuration** button. The appliance is automatically rebooted to apply the changes.

**Rebooting**

You can reboot the Standalone Sentry to clear the current configuration settings and restart all server modules.

**Procedure**

1. In the Standalone Sentry system manager, go to **Maintenance**.
2. Select **Reboot** in the navigation pane.

**FIGURE 1. REBOOTING**

3. Click the **Reboot** button.
Troubleshooting

The following describe the troubleshooting settings in the Standalone Sentry System Manager:

Overview of the Standalone Sentry Troubleshooting tab ................................................................. 131
Logs ................................................................................................................................................. 131
Network Monitor ............................................................................................................................. 136
Service Diagnosis .......................................................................................................................... 138
Sentry Statistics ................................................................................................................................ 139

Overview of the Standalone Sentry Troubleshooting tab

Use the Troubleshooting tab to investigate possible problems with Standalone Sentry operation. In most cases, you will use this tab under the direction of Customer Support.

Table 1. Configuration links in the Troubleshooting tab

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs</td>
<td>Configure and upload log files.</td>
</tr>
<tr>
<td>Network Monitor</td>
<td>Produce a TCP dump for Sentry.</td>
</tr>
<tr>
<td>Service Diagnosis</td>
<td>Check the health of related servers.</td>
</tr>
<tr>
<td>Sentry Statistics</td>
<td>Produce an operational report.</td>
</tr>
</tbody>
</table>

Logs

The Logs page allows you to the following:

- Log management
- View module logs
- Export logs

Log management

You can enable or disable logging and control the details collected in Sentry logs for the following services:

- MICS (MobileIron Configuration Service)
- Sentry
For the Sentry service, you can do the following:

- Specify whether to exclude interactions between Sentry and the device or between Sentry and the backend resource.
- Specify levels of increasing detail.
- Filter logs based on specific attributes, such as Device ID.

**FIGURE 1. TROUBLESHOOTING**

The following table describes the options for managing logs.

**TABLE 1. OPTIONS FOR MANAGING LOGS**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MICS</td>
<td>Includes messages related to the MobileIron Configuration System module that supports the Sentry.</td>
</tr>
<tr>
<td>Sentry</td>
<td>Includes messages related to Sentry operation.</td>
</tr>
<tr>
<td>To/From Device</td>
<td>Includes messages related to interactions between Sentry and the registered ActiveSync devices.</td>
</tr>
</tbody>
</table>
### Table 1. Options for Managing Logs (Cont.)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To/From ActiveSync Server</td>
<td>Includes messages related to interactions between Sentry and the configured ActiveSync servers.</td>
</tr>
<tr>
<td>Level 1</td>
<td>Includes HTTP response/request lines and a few supporting operational messages. This level of provides the least detailed logging.</td>
</tr>
<tr>
<td>Level 2</td>
<td>Includes Level 1 content, HTTP headers, and additional operational messages. Sufficient when network issues are suspected. Primarily used for troubleshooting AppTunnel issues.</td>
</tr>
<tr>
<td>Level 3</td>
<td>Includes Level 1 and Level 2 content and the information associated with the messages. Enabled when you know that there are no network issues, but there may be an issue with ActiveSync. This is the most common level requested by support. The logs contain WBXML. Log data includes email, calendar, and contact information.</td>
</tr>
<tr>
<td>Level 4</td>
<td>Includes all available log data. Enabled if parsing errors or missing data is suspected. Enable, only when requested by Support. Log data includes email, calendar, and contact information.</td>
</tr>
</tbody>
</table>

**Related topics**

- "Turning logging on or off" below
  - "Filtering log entries" on the next page
  - "Disabling filters" on page 135
  - "Deleting filters" on page 135
  - "Viewing logs" on page 135

**Turning logging on or off**

You can turn logging on or off by either selecting or deseleting the MICS or Sentry options under Log Management.
**Procedure**

1. Select or deselect the **MICS** checkbox to turn on or off MICS logging.
2. Select or deselect the **Sentry** checkbox to turn on or off Sentry logging.
3. If you turn on Sentry logging, select log options, level, and filters.
4. Click **Apply**.

**Filtering log entries**

The Filtering section of the Log Management screen enables you to isolate entries based on the following attributes:

- device-id—filters the logs based on the device id
- device-ip—filters the logs based on a specific ip address
- user-id—filters the logs based on a specific user id

User id must be an exact match, but it is case insensitive.

The following example shows how to restrict the display to entries containing user ID johnd.

**Figure 2. Filter Log Entries**

If multiple filters are specified, Sentry performs a logical OR operation; Sentry selects the log lines matching at least one of the filters.

**Procedure**

1. Select the **Enable Filters** checkbox.
2. Click the green + button to display a filter entry.
3. Select an attribute from the **Attribute** drop-down list.
4. In the **Value** field, enter the value you want to match.
   The field is free-form and case-sensitive.
5. In the **Tag Name** field, enter a string that identifies the filter.
   The tag name is added to the log output. Tag names are especially useful when you apply multiple filters.
   Adding a tag name is optional.
6. Click **Apply**.
Disabling filters

Disabling a filter removes the effect of the filter. Select the Disable checkbox to disable the filter. Clear it to re-enable the filter.

Deleting filters

If you do not intend to reuse a filter, you can delete it. To delete a filter, click the red – button.

View logs

The Troubleshooting > Logs page enables you to view the contents of logs directly from the console. Logging must be turned on.

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| MICS     | MobileIron Configuration Service log entries  
Sentry System Manager logs include IP, DNS, debugging, and upgrade configuration. |
| Sentry   | Sentry operation log entries |
| System   | Sentry status log entries |
| Syslog   | A superset of the information in the MICS log  
Includes Sentry system level information and WARN and above application logs. |
| Catalina | Application loading status  
Includes the Sentry application server (tomcat) console logs. |
| Catalina2| Application loading status  
Includes the Sentry System Manager (MICS) application server (tomcat2) console logs. |

Viewing logs

The View Module Logs section in the Troubleshooting > Logs page contains links to logs for Sentry modules.

Procedure

1. In the View Module Logs section, click the link for the log you want to view.
The displayed window shows the most recent log entries. The window scrolls dynamically as the Server adds entries to the log.

2. Click x to close the log view window.

NOTE: If you close the log view window and then re-open it, the displayed window shows only log entries made since you closed the window.

To remove existing log entries from the log view window and view only new log entries, click the Clear Window button.

Exporting logs

The Export Logs section allows you to download logs.

Downloading logs

The following procedure describes how to download Sentry logs. Logs are downloaded to your local drive.

Procedure

1. Go to Troubleshooting > Logs.
2. Scroll down to the Export Logs section.
3. In the Export Logs section, select Download from the Type drop-down list.
4. If you have received a support ticket number associated with this upload, enter it in the Support Ticket Number field.
5. Click Download.

Network Monitor

The Network Monitor page enables you to produce a TCP dump for a Standalone Sentry physical interface. The information provided might assist in troubleshooting device connectivity problems. Click Download to store the results in a pcap file.
Use the following guidelines to complete this screen:

**TABLE 1. NETWORK MONITOR FIELD DESCRIPTIONS**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Select the physical interface for which you want to want to produce a TCP dump. If you have configured multiple interfaces, select <strong>All</strong> to get a TCP dump for all physical interfaces at one time.</td>
</tr>
<tr>
<td>Filter</td>
<td>not implemented.</td>
</tr>
<tr>
<td>Max. packet size</td>
<td>not implemented.</td>
</tr>
<tr>
<td>Max no. of Packets</td>
<td>not implemented.</td>
</tr>
<tr>
<td>Start</td>
<td>Click to start TCP dump. <strong>TIP:</strong> A growing file size indicates that the TCP dump is running.</td>
</tr>
<tr>
<td>Stop</td>
<td>Click to stop TCP dump. <strong>TIP:</strong> Click stop after reproducing the issue.</td>
</tr>
<tr>
<td>Download</td>
<td>Click to download TCP dump. If you click <strong>Download</strong> before starting the TCP dump you may not have any data to download. After starting a TCP dump, you may choose to download later after reproducing the issue. <strong>TIP:</strong> A growing file size indicates that the TCP dump is running.</td>
</tr>
</tbody>
</table>
**Service Diagnosis**

You can use the **Service Diagnosis** page under **Troubleshooting** to check the health of the following services:

- EAS
- NTP
- DNS
- UEM (Core or Cloud)

**Figure 1. Service Diagnosis**

![Service Diagnosis Figure]

Click **Verify All** to recheck the listed services, or click **Verify** next to a specific service to verify just that service.

Clicking **Verify** next to the **UEM** (Core or Cloud) entry causes Standalone Sentry to make another attempt to contact the UEM server. The resulting **Message** field of the **UEM** entry indicates whether the server is reachable.

Some reasons that the UEM may not be reachable include:

- Network errors.
- Actions taken by Technical Support for troubleshooting.

**ActiveSync server status**

You can check the ActiveSync server status by doing one of the following:

- In the Admin Portal, go to **Settings > Service Diagnostic**.
• In the Standalone Sentry System Manager, go to Troubleshooting > Service Diagnosis.

Sentry Statistics

You can download statistics for Sentry operation. These statistics encompass the entire Sentry implementation and all connecting devices. They are most useful for charting true activity peaks so that you can schedule maintenance appropriately. Also, technical support can use these statistics for troubleshooting issues.

When Sentry Statistics is enabled or when Start is selected, the settings persist across Sentry restart. The settings in Sentry Statistics are saved as the following properties in /mi/alcor/config/v2/local/alcor-local.properties:

alcor.local.config.enable.sentry.global.statistics.report=true
alcor.local.config.statistics.log.interval.min=5

Sentry statistics collection is a continuous process. If Sentry statistics is started, the statistics are written to global-stats.csv. When Standalone Sentry restarts, the data is archived.

Use this page for the following:

• Downloading Sentry Statistics
• Viewing Sentry Utilization

FIGURE 1. SENTRY STATISTICS

![Figure 1: Sentry Statistics](image-url)
**Download Sentry Statistics**

Click the Download button to download a ZIP file containing the global statistics and device statistics for the Sentry. The ZIP file contains two CSV files:

- **global-stats.csv**
  Provides overall Sentry statistics, useful for charting peak activity and for troubleshooting.
- **all-device-stats.csv**
  Provides statistics for each device, useful for troubleshooting issues on a specific device.

**Change Statistics collection**

You can make the following changes to Sentry Statistics collection:

- start
- stop
- reset
- change the interval

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Select to start Sentry statistics collection.</td>
</tr>
<tr>
<td></td>
<td>When the <strong>Sentry Statistics</strong> view shows <strong>Start</strong> as selected, statistics</td>
</tr>
<tr>
<td></td>
<td>collection is written to global-stats.csv. This setting is not persistent.</td>
</tr>
<tr>
<td></td>
<td>When Standalone Sentry restarts, the setting defaults to Stop. Statistics</td>
</tr>
<tr>
<td></td>
<td>in global-stats.csv are archived</td>
</tr>
<tr>
<td>Stop</td>
<td>Select to turn off Sentry statistics collection.</td>
</tr>
<tr>
<td></td>
<td>When the <strong>Sentry Statistics</strong> view shows <strong>Stop</strong> as selected, statistics</td>
</tr>
<tr>
<td></td>
<td>collection is no longer written to global-stats.csv.</td>
</tr>
<tr>
<td>Apply &amp; Reset</td>
<td>Click to clear the existing statistics file and restart statistics</td>
</tr>
<tr>
<td>Statistics</td>
<td>collection.</td>
</tr>
</tbody>
</table>

**TABLE 1. STATISTICS COLLECTION OPTIONS**
Changing the log interval

Sentry statistics are recorded to global-stats.csv every 5 minutes by default when statistics collection is enabled. You can change the statistics collection interval.

Procedure
1. Delete the current interval from the Log Interval field.
2. Enter a new interval.
3. Click Apply.

Changes to Snapshot Interval are persistent after a Standalone Sentry restart.

Sentry Utilization

To view the latest Sentry resource utilization information, click Refresh.

There is up to a one minute lag in updating the information.

System utilization alerts

The Standalone Sentry monitors system utilization at 30 minute intervals. An alert is raised if utilization exceeds the default threshold level.

If you configured a syslog server in the Sentry System Manager, these alerts can be made available on the syslog server.

Alerts are generated for the following parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thread Pool Utilization</td>
<td>80%</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>70%</td>
</tr>
<tr>
<td>System Memory Utilization</td>
<td>70%</td>
</tr>
</tbody>
</table>
Monitoring

The following describe the monitoring settings in the Standalone Sentry System Manager:

Overview of the Standalone Sentry Monitoring tab .................................................. 142
Alert Viewer ............................................................................................................. 142
Alert Configuration ................................................................................................. 143

Overview of the Standalone Sentry Monitoring tab

Use the Monitoring tab to view email and AppTunnel alerts. The alerts include, HTTP (email and apps), Kerberos, and ActiveSync status errors. Alerts that are warning and above are shown.

<table>
<thead>
<tr>
<th>TABLE 1. STANDALONE SENTRY MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts Viewer</td>
</tr>
<tr>
<td>Alert Configuration</td>
</tr>
</tbody>
</table>

Alert Viewer

Use this page to view Sentry alerts. Sentry reports multiple types of alerts. Each alert has its own alert ID, and each alert ID is linked to an article in the Knowledge Base if one is available. The Knowledge Base article gives more information on the alert and the related error codes. For ActiveSync traffic, separate alert IDs are provided and each alert ID for ActiveSync traffic corresponds to an ActiveSync command, such as Sync, Ping, or Sendmail, supported by Standalone Sentry.

Note The Following:

- Set the logging level at 3 or more (Sentry System Manager > Troubleshooting > Logs). The Monitoring tab will not show any alerts if logging level is 2 or less.
- The page is not automatically refreshed. Reload the page to refresh the alerts.
- Alerts for ping status 2 are also seen. Ping status 2 is not an error.
- After Standalone Sentry is restarted, only the most recent 1000 lines will be displayed.

Filtering Standalone Sentry alerts

Filtering allows you to narrow down the alerts to a specified set. The filter is applied only to the alerts displayed in the Alert Viewer page.
Procedure

1. In the Standalone Sentry System Manager, go to **Monitoring > Alert Viewer**.

2. Enter a text string in the text box.
   Regular expressions are supported. Case is ignored. Example: Error and ERROR will return the same results.

3. Click **Filter**.
   Only alerts containing the text string are displayed.
   Click **Clear** to clear the filter and return the complete set of alerts.
   Click **Reload** to return an updated set of alerts based on the current filter settings. Reload does not clear the filter. Refreshing the browser will clear the filter.

**Alert Configuration**

Use this page to configure notifications for Standalone Sentry alerts, such as email address to which notifications are sent.
Configuring Sentry alert notifications

Sentry alert notification is configured in the Standalone Sentry System Manager in Monitoring > Alert Configuration.

Procedure
1. In the Sentry System Manager go to Monitoring > Alert Configuration.
2. Use the guidelines in the table to configure notifications.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Notifications</td>
<td>Select the checkbox to enable alert notifications.</td>
</tr>
<tr>
<td>Email List</td>
<td>Enter the email address to send the alerts.</td>
</tr>
<tr>
<td></td>
<td>Enter multiple email addresses as a comma separated list.</td>
</tr>
<tr>
<td>Alerts Per Hour</td>
<td>Enter a number.</td>
</tr>
<tr>
<td></td>
<td>This is the number of alerts in an hour that can be emailed to you.</td>
</tr>
<tr>
<td></td>
<td>For example, if you enter the number 1, you will get one alert once every hour. If there are more than one alerts for that hour, only the first alert is emailed to you. Subsequent alerts within the hour are not emailed. The clock is reset at the top of each hour.</td>
</tr>
<tr>
<td>Batch Time Interval</td>
<td>Enter a number.</td>
</tr>
<tr>
<td>(min.)</td>
<td>Batch notifications are emailed at the interval set in this field.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default</td>
<td>Select the default action for email alert notification. The default action is applied to alerts that do not have a specific email notification action configured.</td>
</tr>
<tr>
<td>Discard</td>
<td>An email notification is not sent for the alerts.</td>
</tr>
<tr>
<td>Realtime Notification</td>
<td>Email notification is sent immediately after the alert. Apply this action to alerts that require immediate attention.</td>
</tr>
<tr>
<td>Batch Notification</td>
<td>Alerts are combined into a single email notification. Use batch notification for non-critical alerts.</td>
</tr>
</tbody>
</table>

3. Click **Apply**.

You must also configure **Email Settings** in the Sentry System Manager to receive alert notifications by email.

### Managing alert notification

Configure a notification action to a Standalone Sentry alert in Monitoring > Alert Notifications in the Standalone Sentry system manager.

**Procedure**

1. In the Alert Notification Management section, click **Add**.
2. In the Add Alert ID pop up, enter an **Alert ID**.
3. From the drop down List, select a notification action.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discard</td>
<td>A notification is not sent for the alert.</td>
</tr>
<tr>
<td>Realtime Notification</td>
<td>Alert notification is sent in real time. Apply this action to alerts that require immediate attention.</td>
</tr>
<tr>
<td>Batch Notification</td>
<td>The Alert is batched into a single notification. Apply this action to non-critical, but important alerts.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.
Command Line Interface

The Standalone Sentry command line reference provides commands to configure many features that are also available in the Standalone Sentry System Manager user interface.

Standalone Sentry CLI also includes commands that are specific to a unified endpoint management (UEM) platform. The UEM platforms are:

- Core
- Cloud

If you execute a UEM platform-specific CLI command in a deployment that does not use that UEM platform, an error message displays.

Example:

```
config# debug sentry check-in
This command is not applicable for the EMM Server
config#
```

The following CLI commands are specific to Standalone Sentry:

- Purging the cache
- Logging
- Configuring garbage collection (GC)
- Monitoring Sentry
- Configuring a syslog server
- Reporting
- Clearing the redirect URL
- Configuring access to UEM
- Enabling and disabling iptables
- curl
- Regenerating the Standalone Sentry self-signed certificate
- Checking Kerberos Key Distribution Center (KDC) connectivity
- Verifying Kerberos configuration
- Initializing Kerberos
- Stopping and restarting Standalone Sentry services
- Configuring kernel parameters
- Using the Splunk forwarder service
- Changing TLS protocols
- Checking TLS compliance
- Enabling and disabling SSL HSTS
- Enabling and disabling web service HSTS
- Upgrading using CLI
Purging the cache

Ivanti does not recommend purging the cache unless required for debugging purposes. These commands are accessible from CONFIG mode.

The purge features available through the CLI are described below:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge the device cache</td>
<td>debug sentry device-cache purge all</td>
</tr>
<tr>
<td>Purge the device cache of a specific device</td>
<td>debug sentry device-cache purge entry &lt;device-id&gt; &lt;user-id&gt;</td>
</tr>
<tr>
<td>Purge the Kerberos cache</td>
<td>debug sentry kerberos-cache purge &lt;upn-string&gt;</td>
</tr>
</tbody>
</table>

- **To purge the device cache**, enter the following command:
  
  ```
  debug sentry device-cache purge all
  ```

  Example of purging the device cache:
  
  ```
  config# debug sentry device-cache purge all
  ```

- **To purge the device cache of a specific device**, enter the following command:
  
  ```
  debug sentry device-cache purge entry <device-id> <user-id>
  ```

  - device-id
    The id of the device for which you want information.
  - user-id
    The User associated with the device.

  Example:
  
  ```
  config# debug sentry device-cache purge entry Appl7S032TF7A4S testuser2674
  ```

- **To purge the Kerberos cache for a specific UPN**, enter the following command:
  
  ```
  debug sentry kerberos-cache purge <upn-string>
  ```

  - upn-string
    The UPN of the Kerberos user for which you want to purge the cached information.

  Example of purging the cache for a Kerberos user:
  
  ```
  config# debug sentry kerberos-cache purge user@ironmobile.com
  ```
Purged 1 entries from cache

Purging CRL cache

You can purge CRL cache entry by using CRL ID:

/usr/bin/curl - XPOST http://localhost:<port>/asproxy/crl-cache?action=purge&amp;crl-id=<crl_id>

Logging

The logging commands are accessible from CONFIG mode. Log configuration is not persistent after a reboot.

The logging features available through the CLI are described below:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Sentry logging</td>
<td>debug sentry log enable {device</td>
</tr>
<tr>
<td>Specify filters</td>
<td>debug sentry log filter &lt;tag&gt;</td>
</tr>
<tr>
<td>Specify verbosity</td>
<td>debug sentry log verbosity {level_1</td>
</tr>
<tr>
<td>Disable Sentry logging</td>
<td>no debug sentry log</td>
</tr>
<tr>
<td>Delete log filters</td>
<td>no debug sentry log filter &lt;tag&gt;</td>
</tr>
<tr>
<td>Disable initialization log messages</td>
<td>no debug sentry init-log</td>
</tr>
<tr>
<td>Enable initialization log messages</td>
<td>debug sentry init-log {level_1</td>
</tr>
</tbody>
</table>

- **To enable Sentry logging**, enter config mode and type the following command:

  `debug sentry log enable {device|server|both}`
  - `device` Optional. Logging is enabled to and from devices.
  - `server` Optional. Logging is enabled to and from the ActiveSync Server.
  - `both` Optional. Logging is enabled to and from both devices and the ActiveSync Server. This value is the default if no parameter is specified.

Example of enabling logging to and from devices:

`config# debug sentry log enable device`

Successful
• **To create a filter**, enter the following command after logging is enabled:

```plaintext
debug sentry log filter <tag> {device-id | device-ip | user-id | bundle-id | service-name | config-uuid} <value>
```

- **tag**
  The tag name that you are assigning to the filter
- **device-id | device-ip | user-id | bundle-id | service-name | config-uuid**
  The attribute—device id, device ip, or user id—that corresponds to this filter
- **value**
  Specify the value of the attribute

Example of creating a filter for a specific user:

```plaintext
config# debug sentry log filter KensDevice user-id ksmith
```

Successful

You can verify that the filter was created by using the following command, in EXEC mode, to view a list of filters:

```plaintext
config# end
#show sentry log filter
```

<table>
<thead>
<tr>
<th>TAG</th>
<th>ENABLED</th>
<th>TYPE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>KensDevice</td>
<td>true</td>
<td>user-id</td>
<td>ksmith</td>
</tr>
</tbody>
</table>

• **To set the log detail level**, enter the following command after logging is enabled:

```plaintext
debug sentry log verbosity {level_1_lowest|level_2|level_3|level_4_highest}
```

- **level_1_lowest**
  Includes HTTP response/request lines and a few supporting operational messages. `level_1_lowest` is the default setting.
- **level_2**
  Includes Level 1 content, HTTP headers, and additional operational messages.
- **level_3**
  Includes Level 1 and Level 2 content and the information associated with the messages.
- **level_4_highest**
  Includes all available log data.

Example of setting the log detail level:

```plaintext
config# debug sentry log verbosity level_1_lowest
```

Successful

• **To disable Sentry logging**, enter the following command:

```plaintext
no debug sentry log
```

Example of disabling the Sentry logging:

```plaintext
config# no debug sentry log
```

Successful

• **To delete Sentry log filters**, enter the following command:

```plaintext
no debug sentry log filter <tag>
```

- **tag**
  The tag of the filter(s) you want to disable.
If there are multiple filters with the same tag, they will all be deleted. To delete or disable specific filters, use the web user interface. For information about deleting filters using the web interface, see "Deleting filters" on page 135. For information about disabling filters using the web interface, see "Disabling filters" on page 135.

Example of deleting filters using the CLI:

```
config# no debug sentry log filter KensPhone
```
Successful

- **To disable log messages during Standalone Sentry initialization**, enter the following command:

```
no debug sentry init-log
```

Example of disabling log messages during Standalone Sentry initialization:

```
config# no debug sentry init-log
```

Restart tomcat service to take this effective.

- **To enable log messages during Standalone Sentry initialization**, enter the following command:

```
debug sentry init-log [level_1_lowest|level_2|level_3|level_4_highest]
```

To set log verbosity, enter one of the following options:

- **level_1_lowest**
  Includes HTTP response/request lines and a few supporting operational messages.
- **level_2**
  Includes Level 1 content, HTTP headers, and additional operational messages.
- **level_3**
  Includes Level 1 and Level 2 content and the information associated with the messages.
- **level_4_highest**
  Includes all available log data. level_4_highest is the default setting.

Example of setting the log detail level:

```
config# debug sentry init-log level_2
```

Restart tomcat service to make this effective.

### Configuring garbage collection (GC)

Garbage Collection (GC) logs are enabled by default. The GC logs are automatically added to show-tech.
### Table 1. Configuring Garbage Collection

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable GC logging and rotation</td>
<td><code>sentry gc-log [file-count] [file-size]</code></td>
</tr>
<tr>
<td><code>file-count</code>: The number of GC log files to use when rotating logs. Enter a number between 1 and 100. The default is 5.</td>
<td></td>
</tr>
<tr>
<td><code>file-size</code>: The size of GC log file at which point the log will be rotated. Enter a file size between 8K and 300M. The default is 20M.</td>
<td></td>
</tr>
<tr>
<td>Disable Sentry GC logging and rotation</td>
<td><code>no sentry gc-log</code></td>
</tr>
<tr>
<td>Requires a restart of Sentry services for changes to take effect.</td>
<td></td>
</tr>
</tbody>
</table>

### Monitoring Sentry

The CLI provide commands to monitor and capture additional information about Sentry server. These commands help debug issues in complex deployments. Enter these commands in CONFIG mode.

The monitoring features include enabling, disabling, port change for packet captures, duration of packet captures, monitoring threads percentage, and monitoring trigger time.

### Table 1. Monitoring Sentry

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Sentry Monitor</td>
<td><code>debug sentry monitor enable</code></td>
</tr>
<tr>
<td>Disable Sentry Monitor</td>
<td><code>no debug sentry monitor enable</code></td>
</tr>
<tr>
<td>Port change for packet captures</td>
<td><code>debug sentry monitor capture port [port_number]</code></td>
</tr>
<tr>
<td>If the port number is not provided, the default port 443 is used.</td>
<td></td>
</tr>
<tr>
<td>Duration of packet captures performed during data collection</td>
<td><code>debug sentry monitor capture time [capture_time]</code></td>
</tr>
<tr>
<td>Capture time is measured in seconds. If <code>capture_time</code> is not provided, the default capture time of 600 seconds is used.</td>
<td></td>
</tr>
<tr>
<td>Sentry server is monitored for the number of running threads over the threshold</td>
<td><code>debug sentry monitor threads percentage [percentage]</code></td>
</tr>
<tr>
<td>If the <code>percentage</code> is not provided, the default value for percentage is 90.</td>
<td></td>
</tr>
<tr>
<td>Sentry monitoring triggers a Sentry restart after the configured time.</td>
<td><code>debug sentry monitor trigger [time_in_minutes]</code></td>
</tr>
<tr>
<td>If the time is not set, the default time of 600 seconds is used.</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a syslog server

Configuring a remote log server to send Sentry syslog data is a two step process and requires the following:

1. "Adding a syslog server" below
2. "Enabling log data" on the next page

To view Sentry facility configuration see:

- "Displaying syslog configuration" on page 154

Adding a syslog server

To add or edit a syslog server, type the following command in CONFIG mode:

```
syslog <server> [port] <protocol> <facility> <log-level> [state]
```

To delete a syslog server, type the following command in CONFIG mode:

```
no syslog <server> [port]
```

Table 1. Adding a syslog server

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server</td>
<td>IP address or hostname of the syslog server.</td>
</tr>
<tr>
<td>port</td>
<td>Syslog server port. Use port 514 if you are adding Monitor. If the port number is not provided, the default port 514 is used.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol of the syslog server. The options are:</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
</tbody>
</table>
### TABLE 1. ADDING A SYSLOG SERVER (CONT.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>facility</td>
<td>Type of log messages sent to the syslog server. The options are:</td>
</tr>
<tr>
<td></td>
<td>• general</td>
</tr>
<tr>
<td></td>
<td>• health-monitor</td>
</tr>
<tr>
<td></td>
<td>• audit</td>
</tr>
<tr>
<td>log-level</td>
<td>Minimum severity level of log messages to be sent. The options are:</td>
</tr>
<tr>
<td></td>
<td>• emerg</td>
</tr>
<tr>
<td></td>
<td>• alert</td>
</tr>
<tr>
<td></td>
<td>• crit</td>
</tr>
<tr>
<td></td>
<td>• err</td>
</tr>
<tr>
<td></td>
<td>• warning</td>
</tr>
<tr>
<td></td>
<td>• notice</td>
</tr>
<tr>
<td></td>
<td>• info</td>
</tr>
<tr>
<td></td>
<td>• debug</td>
</tr>
<tr>
<td></td>
<td>CLI does not limit log-level by the facility choice.</td>
</tr>
<tr>
<td>state</td>
<td>State of the syslog server. The options are:</td>
</tr>
<tr>
<td></td>
<td>• enable</td>
</tr>
<tr>
<td></td>
<td>• disable</td>
</tr>
<tr>
<td></td>
<td>If state is not specified, syslog is enabled by default.</td>
</tr>
</tbody>
</table>

### Enabling log data

After adding a syslog server, you need to also enable the log data for the facility you selected for the syslog server. Sentry forwards the log data that is enabled to the syslog server. General log data is enabled by default. No additional action is required if you chose General facility when you added the syslog server.

To enable log data for the facility, enter the following command in CONFIG mode:

```bash
sentry {audit | health-monitor}
```
### Table 2. Enabling Log Data

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable sentry audit log data</td>
<td>sentry audit</td>
</tr>
<tr>
<td>Enable sentry health monitoring</td>
<td>sentry health-monitor</td>
</tr>
<tr>
<td>Disable sentry audit</td>
<td>no sentry audit</td>
</tr>
<tr>
<td>Disable sentry health monitoring</td>
<td>no sentry health-monitor</td>
</tr>
</tbody>
</table>

### Displaying syslog configuration

To view syslog server facility configuration use the following commands in EXEC or PRIVILEGED mode:

### Table 3. Displaying syslog configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display syslog configuration</td>
<td>show logging</td>
</tr>
<tr>
<td>Display sentry audit configuration</td>
<td>show sentry audit config</td>
</tr>
<tr>
<td>Display sentry health monitoring</td>
<td>show sentry health-monitor</td>
</tr>
</tbody>
</table>

#### Example

```
sentry# show logging
```

```
+---------------------------------------------------------------+
<table>
<thead>
<tr>
<th>Hostname / IP Address + Port + Protocol + Facility Type + Log Level + State</th>
</tr>
</thead>
<tbody>
<tr>
<td>app1111.auto1.mycompany.com 514 UDP health-monitor info enable</td>
</tr>
</tbody>
</table>
```

### Reporting

The CLI provides commands to support the reporting features. The commands are accessible from exec mode.

The reporting features include configuration, cache reporting for systems and devices, statistics for systems and devices, and Kerberos-related reporting.

- "Displaying Sentry configuration" on the next page
- "Displaying information for entries in the device cache" on the next page
Displaying Sentry configuration

You can request a report of the entire configuration or filter by a string of text so that the output only displays rows matching the filter-string text.

To show the Sentry log configuration, enter the following command:

```
show sentry config-properties [filter-string]
```

- filter-string
  Optional. Specify text to filter the output.

Example of a request for output of the Sentry log configuration for asproxy.client:

```
#show sentry config-properties asproxy.client
asproxy.client.port = 80
asproxy.client.tls.port = 443
```

If you do not specify a filter, the output includes all configuration information.

Displaying information for entries in the device cache

You can display information for entries in the Sentry device cache. You can also display information about the in-memory device list, the persistent device list, and connectivity to UEM.

Caution: The purpose of these commands is to assist Technical Support with troubleshooting. Do not depend on the output's format for use with any programs.
**TABLE 1. DISPLAYING INFORMATION FOR ENTRIES IN THE DEVICE CACHE**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display a list of entries in the Sentry device cache.</td>
<td>show sentry device-cache dump {all</td>
</tr>
<tr>
<td>Display detailed information for a specific entry.</td>
<td>show sentry device-cache entry &lt;tunnel-id&gt; &lt;user-id&gt;</td>
</tr>
<tr>
<td>Display the entries associated with a device id</td>
<td>show sentry device-cache device &lt;device-id&gt;</td>
</tr>
<tr>
<td>Display the entries associated with a user id</td>
<td>show sentry device-cache user &lt;user-id&gt;</td>
</tr>
<tr>
<td>Display the entries with the specified number of minimum connections</td>
<td>show sentry device-cache min-connection &lt;value&gt;</td>
</tr>
<tr>
<td>Show the entries that need validation from UEM.</td>
<td>show sentry device-cache validation-pending {yes</td>
</tr>
<tr>
<td>Show the status of the Sentry-device cache.</td>
<td>show sentry device-cache status</td>
</tr>
<tr>
<td>Show the connection status to UEM.</td>
<td>show sentry status</td>
</tr>
</tbody>
</table>

- **To display the entries in the device cache**, type the following command:

  ```
  show sentry device-cache dump {all | active-sync | app-tunnel}
  - all
    Displays all entries in the cache in table format.
  #show sentry device-cache dump all
  - active-sync
    Displays the ActiveSync entries in the cache in table format.
  #show sentry device-cache dump active-sync
  - app-tunnel
    Displays the app tunnel entries in the cache in table format.
  #show sentry device-cache dump app-tunnel
  ```

- **To display detailed information about a specific entry in the device cache**, type the following command:

  ```
  show sentry device-cache entry <tunnel-id> <user-id>
  - tunnel-id
    The Tunnel ID of the entry in the device cache for which you want information. You can view the Tunnel-ID in the output from show sentry device-cache dump.
  - user-id
    The User ID associated with the entry.
  ```
To display all entries associated with a specific device, type the following command:

```bash
show sentry device-cache device <device-id>
```

- **device-id**
  - The device-id for which you want to display all entries.
  - If you provide a partial device id, the rows for all matching devices are displayed.

Example of a request for a report for a specific device-id:

```bash
sentry# show sentry device-cache device 0V55EEVSRT5UVFA05AUBLF904S
```

Index | User       | S | Vs | Cn | Ver | Time                | Application[/ID] |
-----|------------|---|----|----|-----|---------------------|------------------|
1    | testuser3351 | A | Y  | 0  | 14.1 | 2015-08-27 18:30:57 | GMT              |

To display all entries associated with a specific user, type the following command:

```bash
show sentry device-cache user <user-id>
```

- **user-id**
  - The user-id for which you want to display all entries.
  - If you provide a partial userid, the rows for all matching users are displayed.

Example of a request for a report for a specific user-id:

```bash
sentry# show sentry device-cache user testuser3351
```

Index | User       | S | Vs | Cn | Ver | Time                | Application[/ID] |
-----|------------|---|----|----|-----|---------------------|------------------|
1    | testuser3351 | A | Y  | 0  | 14.1 | 2015-08-27 18:30:57 | GMT              |
To display the entries with the specified minimum number of connections, enter the following command:

```
show sentry device-cache min-connection <value>
```

Value

The number of connections, at a minimum, for which you want to display the associated entries.

Example of a request for a list of devices that have the minimum number of connections:

```
#show sentry device-cache min-connection 1
```

To display the entries that require EMM validation, enter the following command:

```
show sentry device-cache validation-pending {yes | no}
```

Example of a request for a list of devices that require validation from UEM:

```
#show sentry device-cache validation-pending yes
```

To display information about the persistent device list and the in-memory device list, enter the following command:

```
show sentry device-cache status
```

Example of the command:

```
#show sentry status
EMM server type : Core
Connectivity to Core : Connected
   Last connectivity change detected by : Periodic connectivity check
   Last connectivity change time : Fri Aug 03 18:55:16 UTC 2012

Core periodic connectivity check status
   Current time : Fri Aug 03 21:32:49 UTC 2012
   Last successful : Fri Aug 03 21:25:17 UTC 2012
   Last failed : Never
   Next scheduled : Fri Aug 03 21:40:17 UTC 2012

EMM server fail-open status : Allow
   Last fail-open status change detected by : Sentry initialization
   Last fail-open status change time : Tue Aug 02 23:05:08 UTC 2012
```

The Standalone Sentry detects changes to EMM connectivity in one of the following ways:
- The Standalone Sentry checks EMM connectivity on a regular basis. This is known as the periodic connectivity check.
- The Standalone Sentry checks EMM connectivity when the Sentry initializes.
- The administrator can manually check EMM connectivity by using the Verify button on the Troubleshooting > Service Diagnosis page of the Standalone Sentry Web Portal.

### Displaying information about Kerberos modules

You can display the Kerberos and UPN information. The new CLI commands for Kerberos reporting are described below.

**Table 2. Displaying information about Kerberos modules**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the SPN, timeout, and cache size for Kerberos</td>
<td>show sentry kerberos</td>
</tr>
<tr>
<td>Display Kerberos UPN information</td>
<td>show sentry kerberos cache dump [upn-filter]</td>
</tr>
<tr>
<td>Display Kerberos information related to a specific UPN</td>
<td>show sentry kerberos cache upn &lt;upn-string&gt;</td>
</tr>
</tbody>
</table>

- **To display Kerberos information for the Sentry**, enter the following command:

  ```
  show sentry kerberos
  ```

  Example of a request for Kerberos information:

  ```
  # show sentry kerberos
  sentry-spn = HTTP/sentry.company.com
  cache-ticket-idle-timeout = 48
  cache-size = 1
  ```

- **To display information for all UPNs in the Kerberos cache**, enter the following command:

  ```
  show sentry kerberos cache dump [upn-filter]
  ```

  - upn-filter
    Optional. Full or partial UPN to filter on. Shows only the rows matching this string.

  Example of a request to display Kerberos UPN information for UPNs that match the upn-filter:

  ```
  # show sentry kerberos cache dump user
  Indx  User-UPN         Created(m)  IdleTime(m)
  1    user@ironmobile.com   1010        7
  ```

- **To display Kerberos information for a specific UPN in the Kerberos cache**, enter the following command:

  ```
  show sentry kerberos cache upn <upn-string>
  ```

  - upn-string
    The full UPN of the UPN for which you want to display information.
Example of a request to display Kerberos UPN information for a specific UPN:

```
# show sentry kerberos cache upn user@ironmobile.com
Kerberos Cache for UPN: user@ironmobile.com
  [0] user-upn = user@ironmobile.com
  [0] idle-time-min = 7
  [0] creation-time = Fri Jan 13 01:44:11 UTC 2012
```

### Displaying Sentry statistics

Displays statistics for Sentry. You can specify parameters for global statistics or statistics for a specific device.

**Table 3. Displaying Sentry Statistics**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Sentry statistics for a specific device</td>
<td>show sentry statistics entry <code>&lt;device-id&gt; &lt;user-id&gt;</code></td>
</tr>
<tr>
<td>Display Sentry global statistics for a specific device</td>
<td>show sentry statistics global <code>[device]system [filter-string]</code></td>
</tr>
<tr>
<td>Display complete global Sentry system statistics</td>
<td>show sentry statistics global system <code>[filter-string]</code></td>
</tr>
<tr>
<td>Display complete global Sentry statistics for a server</td>
<td>show sentry statistics global server <code>[filter-string]</code></td>
</tr>
</tbody>
</table>

- **To display complete Sentry statistics for a specific device**, type the following command:

```
show sentry statistics entry `<device-id> <user-id>`
  - device-id
    - The id of the device for which you want information.
  - user-id
    - The User associated with the device.

Example:
sentry# show sentry statistics entry App1DN6FM6SZDKPH testuser2885
d-connection = 4
s-connections = 4
d-bytes-rcvd = 8572
s-bytes-sent = 8368
s-bytes-rcvd = 2704
d-bytes-sent = 2704
d-http-requests = 20
s-http-requests = 16
s-http-responses = 16
d-http-responses = 16
```
d-http-449 = 0
s-http-449 = 0
permits = 16
pendings = 0
blocks = 0
wipes = 0
s-http-3xx-redirects = 0
s-http-451-redirects = 0
d-http-451-redirect-drops = 0
cmd-none = 0
cmd-options = 0
cmd-provision = 0
cmd-sync = 0
cmd-folder-sync = 0
cmd-ping = 16
cmd-get-attachment = 0
cmd-item-operations = 0
cmd-unknown = 0
d-err-conn-timeout = 0
s-err-conn-timeout = 0
d-err-so-timeout = 0
s-err-so-timeout = 0
s-err-cmd-ping-timeout = 0
s-err-cmd-sync-timeout = 0
d-err-cmd-timeout = 0
s-err-cmd-timeout = 0
d-err-reset = 0
s-err-reset = 0
d-so-close = 0
s-so-close = 0
http-status-200 = 0
http-status-401 = 16
http-status-404 = 0
http-status-409 = 0
http-status-5xx = 0
http-status-other = 0
err-conn-pooling = 0
d-unclassified = 0
s-unclassified = 0
ping-sync-throttled = 0
kerberos-auth-error = 0
• **To display complete global Sentry statistics for devices**, type the following command:

```
show sentry statistics global device <filter-string>
- filter-string
    The full or partial string of one of the fields in the statistics report. The filter-string can either be a field name or a value in the field.
```

Example of a request to display global statistics for devices, filtered on http-status:

```
# show sentry statistics global device http-status
http-status-200 = 388
http-status-401 = 32
http-status-404 = 0
http-status-409 = 0
http-status-5xx = 0
http-status-other = 0
```

• **To display complete global Sentry system statistics**, type the following command:

```
show sentry statistics global system [filter-string]
- filter-string
    The full or partial string of one of the fields in the statistics report. The filter-string can either be a field name or a value in the field.
```

Example of a request to display global Sentry statistics, filtered on peak:

```
# show sentry statistics global system peak

peak-heap-mem-used-MB = 389
```
The full global statistics report can be downloaded in CSV format using the user interface. See "Sentry Statistics" on page 139.

- To display complete global Sentry statistics for a server, type the following command:

```
show sentry statistics global server <filter-string>
```

- filter-string
  The full or partial string of one of the fields in the statistics report. The filter string can either be a field name or a value in the field.

Example:

```
sentry# show sentry statistics global server
hc-connections = 6
hc-bytes-sent = 816
hc-bytes-rcvd = 1116
hc-http-requests = 6
hc-http-responses = 6
hc-err-conn-timeout = 0
hc-err-so-timeout = 0
hc-err-reset = 0
hc-so-close = 0
hc-unclassified = 0
hc-http-status-200 = 0
hc-http-status-401 = 6
```
hc-http-status-404 = 0
hc-http-status-other = 0

Example with filter string:
sentry#show sentry statistics global server err
hc-err-conn-timeout = 0
hc-err-so-timeout = 0
hc-err-reset = 0
sentry#

**Displaying information about servers**

- To display server details and connection status, type the following command in EXEC mode:

  ```
  show sentry server status
  Example:
  sentry# show sentry server status
  ```

  **Current Time : Thu Aug 27 19:21:37 UTC 2015**

  **Service Name : <ANY>**
  **Service Type : App Tunnel**
  **Server Scheduling : PRIORITY**

<table>
<thead>
<tr>
<th>Server Name/IP</th>
<th>Declared Last</th>
<th>Failure Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live</td>
<td>Never</td>
<td>0</td>
</tr>
</tbody>
</table>

  **Service Name : default**
  **Service Type : Active-Sync**
  **Server Scheduling : PRIORITY**
  **Active Background Health Check : Enabled**

<table>
<thead>
<tr>
<th>Server Name/IP</th>
<th>Declared Last</th>
<th>Last Status</th>
<th>Successful</th>
<th>Failed</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>ex2010sp3.enterprise.com</td>
<td>Live</td>
<td>08/27/2015 19:20:52</td>
<td>Never</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

  **Service Name : <TCP_ANY>**
  **Service Type : App Tunnel**
  **Server Scheduling : PRIORITY**
<table>
<thead>
<tr>
<th>Name/IP</th>
<th>Status</th>
<th>Failed</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Live</td>
<td>Never</td>
<td>0</td>
</tr>
</tbody>
</table>

sentry#

**Displaying Sentry system resources**

- To display Sentry system resources, type the following command:

  ```bash
  show sentry utilization
  ```

  Example:

  ```bash
  sentry#show sentry utilization
  Number of Connected Devices : 0
  Number of Open Connections  : 0
  Thread Pool Utilization     : 0.0%
  CPU Utilization             : 0%
  System Memory Utilization   : 23%
  Heap Memory Utilization     : 15%
  ```

sentry#

**Displaying Sentry log configuration**

You can display the Sentry log configuration. To change the log configuration, see the commands in "Logging" on page 148.

To display the Sentry log configuration, type the following command:

  ```bash
  show sentry log
  ```

Example of a request to display log configuration information:

```bash
# show sentry log
    log-from-to = both
    enable = true
    verbosity = level3
```

**Displaying Sentry log filters**

You can display the log filters that are currently configured on Sentry. To configure the log filters, see "Logging" on page 148.

To display the Sentry log filters, type the following command:

  ```bash
  show sentry log filter
  ```
Example of a request to display the log filters:

```
# show sentry log filter
TAG    ENABLED TYPE     VALUE
KensPhone  true  user-id  ksmith
```

### Displaying Sentry GC log configuration

You can display the garbage collection (GC) currently configured on Sentry. To configure GC, see "Configuring garbage collection (GC)" on page 150.

To display the Sentry GC configuration, type the following command:

```
show sentry gc-log
```

### Clearing the redirect URL

To clear a redirect URL from the Sentry, enter the following command:

**Table 1. Clearing the redirect URL**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear redirect URL</td>
<td>debug sentry device-cache clear-redirect-url (all</td>
</tr>
</tbody>
</table>

To clear the redirect URL for a specific device, enter the following CLI command:

```
debg sentry device-cache clear-redirect-url entry <device-id> <user-id>
```

- `<device-id>`
  - The device id of the device for which you want to delete the redirect URL.

- `<user-id>`
  - The User associated with the device.

Example:

```
sentry/config# debug sentry device-cache clear-redirect-url entry App175032TF7A4S testuser2674
sentry/config#
```

To clear the redirect URL for all devices, enter the following CLI command:

```
debg sentry device-cache clear-redirect-url all
```
Example

```
sentry/config# debug sentry device-cache clear-redirect-url all
```

## Configuring access to UEM

To configure new device access to the UEM server when the UEM server is not reachable, enter one of the following commands:

### Table 1. Configuring access to UEM

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow new devices to access the server.</td>
<td>sentry emm-fail-open</td>
</tr>
<tr>
<td>Block new devices from accessing the server.</td>
<td>no sentry emm-fail-open</td>
</tr>
</tbody>
</table>

- **To allow new devices to access the server when the UEM server is not reachable**, type the following command in CONFIG mode:

```
sentry emm-fail-open
```

Example:

```
sentry/config# sentry emm-fail-open
sentry/config#
```

- **To block new devices from accessing the server when the UEM server is not reachable**, type the following command in CONFIG mode:

```
no sentry emm-fail-open
```

Example:

```
sentry/config# no sentry emm-fail-open
sentry/config#
```

## Enabling and disabling iptables

The iptables service is enabled by default. Any changes to the configuration is persistent. A write is not required to save any changes in the configuration.

- **If the iptables service is disabled, you cannot configure ACLs in the Sentry System Manager.**

To enable or disable the iptables service at system startup, enter one of the following commands in CONFIG mode:
Table 1. Enabling and Disabling iptables

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the iptables service.</td>
<td>service iptables enable</td>
</tr>
<tr>
<td>Disable the iptables service.</td>
<td>no service iptables</td>
</tr>
</tbody>
</table>

- To enable the iptables service, type the following command in CONFIG mode:

```bash
service iptables enable
```

Example:
```
sentry/config# service iptables enable
sentry/config#
```

- To disable the iptables service, type the following command in CONFIG mode:

```bash
no service iptables
```

Example:
```
sentry/config# no service iptables
sentry/config#
```

- To view whether the iptables service is enabled or disabled at system startup, type one of the following commands in EXEC mode:

```bash
show service
```

or

```bash
show running-config
```

Example:
```
sentry#show service
+-----------------------------+
<table>
<thead>
<tr>
<th>Servicename</th>
<th>Enabled</th>
<th>Max.Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh</td>
<td>yes</td>
<td>5</td>
</tr>
<tr>
<td>ntp</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>iptables</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>
```

Example:
```
sentry#show running-config
Display running configuration
interface GigabitEthernet 1
  ip address 10.10.27.14 255.255.0.0
  no shutdown
end
interface GigabitEthernet 2
  no ip address
```
shutdown
end
interface GigabitEthernet 3
  no ip address
  shutdown
end
interface GigabitEthernet 4
  no ip address
  shutdown
end
ip route 0.0.0.0 0.0.0.0 10.10.1.1
no dbconfig
service ssh 5
service ntp
no service iptables
ip name-server 10.10.15.6 0
ip name-server 10.11.50.31 1
ip domain-name auto.mobileiron.com
ntp 172.16.0.235 1
hostname app264.auto.mobileiron.com
timeout 0
system user miadmin ***
sentry#

• To view the iptables service status, type the following command in EXEC PRIVILEGED mode:

  #service iptables status

  Example:

  sentry# service iptables status

curl

A new curl CLI command is added to allow you to run cURL operation from EXEC Privileged mode.

The cURL features available through CLI are described in the following table:
**TABLE 1. CURL COMMANDS**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>cURL to the ActiveSync destination server</td>
<td><code>curl active-sync &lt;dest&gt; [port] [scheme] [protocol] &lt;user&gt;</code></td>
</tr>
<tr>
<td>cURL to the AppTunnel destination server</td>
<td><code>curl app-tunnel &lt;dest&gt; [port] [method] [scheme] [protocol] [user]</code></td>
</tr>
</tbody>
</table>

- **To cURL to the ActiveSync destination server**, enter the following command:

  `curl active-sync <dest> [port] [scheme] [protocol] [user]`
  - dest Required. The IP address or hostname of the destination server.
  - port Optional. The port for the destination server. The default used is 443.
  - scheme Optional. The HTTP scheme. Enter HTTP or HTTPS. The default used is HTTPS.
  - protocol Optional. The SSL protocol version. Enter TLSv1, or SSLv2. The entry is ignored if SSL is not required. The default used is TLSv1.
  - user Optional. Enter the username for the destination server.

  Example:
  
  #curl active-sync activesyncserver.domainname.com

- **To cURL to the AppTunnel destination server**, enter the following command:

  `curl app-tunnel <dest> [port] [method] [scheme] [protocol] [user]`
  - dest Required. The IP address or hostname of the destination server.
  - port Optional. The port for the destination server. The default used is 443.
  - method Optional. The HTTP method. Enter GET, HEAD, or OPTIONS. The default used is GET.
  - scheme Optional. The HTTP scheme. Enter HTTP or HTTPS. The default used is HTTPS.
  - protocol Optional. The SSL protocol version. Enter TLSv1, or SSLv2. The entry is ignored if SSL is not required. The default used is TLSv1.
  - user Optional. Enter username for the destination server.

  Example:
  
  #curl app-tunnel appserver.domainname.com
Regenerating the Standalone Sentry self-signed certificate

You can regenerate the Standalone Sentry self-signed certificate using the command line interface (CLI). You can regenerate only the self-signed certificate or both self-signed and CA certificates.

Impact of regenerating the Standalone Sentry self-signed certificate

Regenerating the self-signed certificate will impact email and app tunnel deployments. The self-signed certificate will have to be re-pushed to the devices.

Regenerating the CA certificate, in addition, impacts Tunnel. For Tunnel, the CA certificate must be manually uploaded to the device.

How to regenerate the Standalone Sentry self-signed certificate

To regenerate the Standalone Sentry certificates, enter the following CLI command in configuration mode:

certificate {portal}

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regenerate Standalone Sentry self-signed portal certificate</td>
<td>certificate portal</td>
</tr>
</tbody>
</table>

To regenerate Standalone Sentry self-signed portal certificate, enter the following CLI command:

certificate portal

Example

```
config# certificate portal
Services will be disrupted.
Would you like to proceed? [y/n]:
```

If Standalone Sentry does not use a self-signed certificate

If Standalone Sentry does not use a self-signed certificate, then the `certificate {portal | sentry}` command will return the following message:

"Non Self-Signed Certificate in use. No Action performed"
Checking Kerberos Key Distribution Center (KDC) connectivity

To check connectivity and reachability to a KDC host use the following CLI command:

```
dbgsent kerberos kdc
```

This allows you to check that the port on the KDC host is reachable and ensure that the port is not blocked by firewall.

Executing the `dbgsent kerberos kdc` CLI command causes a TCP connection to the specified KDC host. If a port is not specified, the default KDC port 88 is used. The TCP connection is dropped immediately after establishing a connection without either sending or receiving any data.

Checking connectivity to a KDC host

To check connectivity to a KDC host, enter the following CLI command in configuration mode:

```
dbgsent kerberos kdc <hostname> [port]
```

- **hostname**
  The hostname for the KDC server.

- **port**
  The port for the KDC server. If port is not specified, the default port 88 is used.

**Successful example**

```
sentry/config# dbgsent kerberos kdc win2k8.acmetwo.acme.com
Connecting to KDC win2k8.acmetwo.acme.com, port 88
Connection successful.
Address: win2k8.acmetwo.acme.com/192.0.2.0:88
sentry/config#
```

**Failure example**

```
sentry/config# dbgsent kerberos kdc win2k8.acmeone.acme.com
Connecting to KDC win2k8.acmeone.acme.com, port 88
Connection failed.
java.net.UnknownHostException: win2k8.acmeone.acme.com
    at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:184)
    at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392)
    at java.net.Socket.connect(Socket.java:589)
    at java.net.Socket.connect(Socket.java:538)
    at java.net.Socket.<init>(Socket.java:434)
```
Verifying Kerberos configuration

To verify the Keberos constrained delegation (KCD) setup, use the following CLI command:

```
debug sentry kerberos request-ticket
```

The CLI command issues a Kerberos ticket for a particular user. These tickets are issued for testing and debugging only and are not cached or reused.

**TABLE 1. Verifying Kerberos configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request a kerberos ticket on behalf of a user with a host:port combination</td>
<td>debug sentry kerberos request-ticket host-port &lt;upn&gt; &lt;realm&gt; &lt;hostname&gt; [port]</td>
</tr>
<tr>
<td></td>
<td>• upn: user’s UPN</td>
</tr>
<tr>
<td></td>
<td>• realm: user’s REALM</td>
</tr>
<tr>
<td></td>
<td>• hostname: backend server’s hostname</td>
</tr>
<tr>
<td></td>
<td>• port:: backend server’s port</td>
</tr>
<tr>
<td></td>
<td>The default value for port is 443.</td>
</tr>
<tr>
<td>Request a kerberos ticket on behalf of a user with an SPN</td>
<td>debug sentry kerberos request-ticket spn &lt;upn&gt; &lt;realm&gt; &lt;spn&gt;</td>
</tr>
<tr>
<td></td>
<td>• upn: user’s UPN</td>
</tr>
<tr>
<td></td>
<td>• realm: user’s REALM</td>
</tr>
<tr>
<td></td>
<td>• spn: service principal name</td>
</tr>
</tbody>
</table>

Initializing Kerberos

To initialize Keberos, use the following CLI command:

```
debug sentry kerberos init
```

The CLI command initializes Kerberos. If Kerberos is already initialized, executing the command has not impact.
Stopping and restarting Standalone Sentry services

You can stop, start, or restart the following Standalone Sentry services from the Standalone Sentry command line interface (CLI):

- iptables
- tomcat
- tomcat2

Restarting a service, stops the service and then restarts the service automatically.

**Table 1. Stopping and restarting Standalone Sentry services**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop a service</td>
<td>`service (iptables</td>
</tr>
<tr>
<td>Start a service</td>
<td>`service (iptables</td>
</tr>
<tr>
<td>Restart a service</td>
<td>`service (iptables</td>
</tr>
<tr>
<td>View service status</td>
<td>`service (iptables</td>
</tr>
</tbody>
</table>

This allows the administrator to stop, start, or restart a Standalone Sentry service without having to reboot Standalone Sentry and prevents disruption to other services that are running.

Impact of stopping and restarting Standalone Sentry services

- Stopping or restarting tomcat2 will impact access to Standalone Sentry system manager UI and CLI commands. The Standalone Sentry system manager will not be available and you will be able to execute only a subset of the CLI commands.
- Stopping or restarting tomcat or iptables services will impact Standalone Sentry traffic till the service is back up and running.
- After stopping a service through the CLI, restarting Standalone Sentry also restarts the service.

How to stop and restart Standalone Sentry services

- **To stop a service**, enter the following command:

  `service [iptables | tomcat | tomcat2] stop`

  Example for stopping tomcat:

  `sentry# service tomcat stop`
• **To start a service**, enter the following command:

```
service [iptables | tomcat | tomcat2] stop
```

Example for starting tomcat::
```
sentry# service tomcat start
```

• **To restart a service**, enter the following command:

```
service [iptables | tomcat | tomcat2] restart
```

Example for restarting tomcat::
```
sentry# service tomcat restart
```

• **To view service status**, enter the following command:

```
service [iptables | tomcat | tomcat2] status
```

Example for viewing tomcat::
```
sentry# service tomcat status
```

## Configuring kernel parameters

To configure kernel parameters, enter the following command in CONFIG mode:

```
kparam {rp_filter | log_martians | kernel_panic | tcp_sack | tcp_keepalive_time | tcp_keepalive_probes | tcp_keepalive_intvl} [kvalue]
```

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set this value to filter the kernel parameters.</td>
<td>kparam rp_filter [kvalue]</td>
</tr>
<tr>
<td>kvalue is 0, 1 or 2.</td>
<td></td>
</tr>
<tr>
<td>Set this value to allow any unsigned integer value.</td>
<td>kparam log_martians [kvalue]</td>
</tr>
<tr>
<td>kvalue is 0 or 1.</td>
<td></td>
</tr>
<tr>
<td>Set this value to allow safe recovery of any kernel malfunction.</td>
<td>kparam kernel_panic [kvalue]</td>
</tr>
<tr>
<td>kvalue is an integer equal to or greater than 0.</td>
<td></td>
</tr>
<tr>
<td>Set this value to configure TCP SACK.</td>
<td>kparam tcp_sack [kvalue]</td>
</tr>
<tr>
<td>kvalue is kvalue is 0 or 1.</td>
<td></td>
</tr>
</tbody>
</table>
Using the Splunk forwarder service

You can enable and perform other actions for the Splunk forwarder service from the Standalone Sentry command line interface (CLI).

The following table lists the commands.

<table>
<thead>
<tr>
<th><strong>Table 1. Splunk forwarder service CLI commands in Standalone Sentry</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
</tr>
<tr>
<td>Enable the Splunk forwarder service</td>
</tr>
<tr>
<td>Disable the Splunk forwarder service</td>
</tr>
<tr>
<td>Start Splunk forwarder service</td>
</tr>
<tr>
<td>Stop Splunk forwarder service</td>
</tr>
<tr>
<td>Status of the Splunk forwarder service</td>
</tr>
<tr>
<td>Restart the Splunk forwarder service</td>
</tr>
<tr>
<td>Verify if the service is enabled or disabled</td>
</tr>
</tbody>
</table>

Changing TLS protocols

To change the TLS protocol version, use the following CLI command in CONFIG mode:

```
httpd protocol protocol-list
```

You can configure the following TLS versions:

- TLSv1
- TLSv1.1
- TLSv1.2.

Enter the versions as a comma-separated list. The updates will be applied to port 8443 and 9090 only. By default, TLSv1 is disabled and TLSv1.1 and TLSv1.2 are enabled on ports 8443 and 9090.

Example:

```
sentry/config# httpd protocol tlsv1.1,tlsv1.2
Changes will issue restart of httpd service and Sentry system service might be disturbed. Would you like to proceed? [y/n]: y
sentry/config# do show httpd protocol
```
Checking TLS compliance

For improved security, Ivanti recommends that TLS v1.2 is used and TLS v1.0 and v1.2 are disabled. You can check which servers that Sentry connects with support TLS v1.2 using one of the following methods from the Standalone Sentry command line interface (CLI):

- "Using CLI command to check TLS compliance" below
- "Running TLS compliance utility" on the next page

Both methods return an OK or FAILED value for each server that is checked.

OK indicates that Standalone Sentry is able to successfully connect with the server on TLS v1.2.

FAILED indicates that Standalone Sentry cannot connect with the server on TLS v1.2.

The results are also recorded into a log file /var/log/TLSTrafficTool-timestamp.log. The log file is included in ShowTech-All. In case of failure, additional error message content as provided by OpenSSL displays and is recorded in the log file. Ivanti recommends upgrading the failed servers to support TLS v1.2.

Using CLI command to check TLS compliance

You can use a CLI command instead of the utility.

Use the following Standalone Sentry command in EXEC PRIVILEGED mode to check TLS compliance:

```
tlscheck {all | server <server> [port]}
```

The command checks the servers that Sentry connects with and returns an OK or FAILED value for each server it checks.

To check TLS compliance for all servers that Standalone Sentry connects with, enter the following command:

```
tlscheck all
```

To check TLS compliance for specified servers that Standalone Sentry connects with, enter the following command:

```
tlscheck server server [port]
```
where:

- *server* is the IP address or the hostname of the server
- *port* is the port on which the server listens. If the port is not specified, 443 is used.

**Running TLS compliance utility**

Ivanti provides an utility that you can execute from the Standalone Sentry CLI that checks if Sentry can successfully connect with the server on TLS v1.2.

From the Standalone Sentry command line interface, enter the following command in EXEC PRIVILEGED mode:

```bash
#install rpm url url_for_the_rpm
```

The command executes a script that checks the servers that Sentry connects with and returns an OK or FAILED value for each server it checks. The script uninstalls after each run.

**Enabling and disabling SSL HSTS**

Enabling HSTS (RFC 6797) enforces secure HTTPS connection between a web browser and Standalone Sentry. By default, HSTS is disabled.

Before enabling HSTS ensure the following:

- Standalone Sentry uses a root or intermediate certificate from a publicly trusted CA.
- You have policies and processes to ensure that the certificate is current.
- Port 443 is open.

To enable SSL HSTS, use the following CLI command in CONFIG mode:

```bash
httpd hsts enable
```

If HSTS is enabled, the following header is added to the HTTP response:

```
Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

To disable SSL HSTS, use the following CLI command in CONFIG mode:

```bash
no httpd hsts
```
After disabling HSTS, also clear HSTS for the Standalone Sentry FQDN from your browser cache. Otherwise, the browser continues to attempt to load the Standalone Sentry FQDN with a secure connection and you will not be able to access the site.

To view the current status of SSL HSTS, use the following CLI command in EXEC mode:

```
show httpd hsts
```


## Enabling and disabling web service HSTS

Enabling HSTS (RFC 6797) enforces secure HTTPS connection between web services that talk to the web browsers and Standalone Sentry. By default, HSTS is Enabled.

Restart Tomcat for enable/disable HSTS operations to take effect.

Before enabling HSTS ensure the following:

- Standalone Sentry uses a root or intermediate certificate from a publicly trusted CA.
- You have policies and processes to ensure that the certificate is current.
- Port 443 is open.

- To enable HSTS, use the following CLI command in CONFIG mode:
  - `sentry hsts enable`

- To disable HSTS, use the following CLI command in CONFIG mode:
  - `no sentry hsts`

- To show HSTS in the current setting, use the following CLI command in CONFIG mode:
  - `do show sentry hsts`
- To view the current status of HSTS, use the following CLI command in EXEC mode:
  - `show sentry hsts`

**Examples**

- **Enabling HSTS**

  `sentry@app431.auto.ivanti.com/config# sentry hsts enable`
  
  Are you sure you want to enable Sentry Strict-Transport-Security (HSTS rfc6797)? {yes|[no]} : yes

  Please restart tomcat service for changes to take effect.
  `sentry@app431.auto.ivanti.com/config#`

- **Disabling HSTS**

  `sentry@app431.auto.ivanti.com/config# no sentry hsts`

  Disabling Strict-Transport-Security (HSTS rfc6797) for Sentry.
  Please restart tomcat service for changes to take effect.
  `sentry@app431.auto.ivanti.com/config#`


**Upgrading using CLI**

The following describe the steps for upgrading the Standalone Sentry version using CLI:

1. "Configuring your update repo" below
2. "Initiating the upgrade" on the next page
3. "Rebooting Standalone Sentry" on the next page
4. "Verifying that the upgrade is complete" on the next page

**Configuring your update repo**

The following procedure describes the steps to update the repo.

**Procedure**

1. Log into the Standalone Sentry command line interface (CLI) using the administrator account you created during installation.
2. Enter the following command to switch to EXEC Privileged mode:
   
   `enable`
3. Enter the password for enabling the EXEC Privileged mode.
   
   The command line prompt changes:
   
   `#`
4. Enter the following command to enable CONFIG mode:
   
   `configure terminal`
5. Enter the following command to specify the URL and credentials for the repo:
software repository https://support.mobileiron.com/mi/sentry/<version>/ <username> <password>
where <username> and <password> are your company's software download/documentation credentials as provided by Support.
For the upgrade URL, see the Standalone Sentry Release Notes for the release.

NOTE:
- The CLI upgrade will to fail if the trailing ‘/’ after the version number is missing.
  Example: Enter ...sentry/9.13.0/
  If the trailing ‘/’ is missing, you will see the following error message:
  Unable to find applicable update packages in software repository. Please check URL.

6. Enter the following command to exit CONFIG mode:
   end

Initiating the upgrade

The following procedure describes the steps to initiate the upgrade.

Procedure
1. In EXEC Privileged mode enter the following command:
   software checkupdate
2. Confirm that there are no errors displayed.
3. Enter the following command to download the latest available updates:
   software update

Rebooting Standalone Sentry

The following procedure describes the steps to reboot Standalone Sentry.

Procedure
1. After all the listed updates are installed, in EXEC Privileged mode, enter the following command to reload
   the appliance:
   reload
   The following message displays:
   System configuration may have been modified. Save? [yes/no]
2. Enter yes.
   The following message displays:
   Proceed with reload? [yes/no]
3. Enter yes.

Verifying that the upgrade is complete

The following procedure describes the steps to verify the upgrade.
Procedure

In EXEC Privileged mode enter:

```
show version
```

The Sentry Standalone version should be the version to which you upgraded.

**Configuring a proxy server for upgrades**

In cases where you may have a proxy server sitting between Standalone Sentry and support.mobileiron.com, you can configure the upgrade to go through the proxy server. The following table describes the commands for configuring a proxy server for software upgrades:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command in CONFIG mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a proxy server for software upgrades</td>
<td>software outbound-proxy &lt;hostname&gt; &lt;port&gt; [username] [password]</td>
</tr>
<tr>
<td></td>
<td>•  hostname: The hostname or IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>•  port: Port number on the proxy server for Sentry.</td>
</tr>
<tr>
<td></td>
<td>•  username: Username to authenticate to the proxy server if authentication is required.</td>
</tr>
<tr>
<td></td>
<td>•  password: Password to authenticate to the proxy server if authentication is required.</td>
</tr>
<tr>
<td>Disable proxy server configuration</td>
<td>no software outbound-proxy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Command in EXEC or PRIVILEGED mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display proxy server information</td>
<td>show software outbound-proxy</td>
</tr>
</tbody>
</table>

Example for configuring a proxy server for software upgrades:

```
sentry/config# software outbound-proxy proxyserver.company.com 8080
```

**Upgrading multiple Sentry**

You can upgrade multiple Standalone Sentry at the same time using the Sentry CLI.
Before you begin

- Download the upgradeConfig.json file from the support site to a location where Standalone Sentry can access the file.
- Edit the upgradeConfig.json file with the following details:
  - targetVersion: Enter the version of the Sentry that you want to upgrade to.
  - emailTo: Enter the email (comma separated email IDs) to receive upgrade notifications.
  - sentryGroup: Group the existing Sentrys in your deployment.
  - sentryList (on-prem): Enter the FQDN of the Sentry that you want to upgrade.
  - sentryList (cloud): Enter the IP Address for the Sentry on cloud that you want to upgrade.
  - sentryUpgradeGroupList: Enter the Sentry groups that you want to upgrade.

Procedure

1. Log into the CLI using the administrator account you created during installation.
2. Enter the following command to switch to EXEC Privileged mode:
   ```
   enable
   ```
3. Enter the password for enabling the EXEC Privileged mode.
   The command line prompt changes:
   ```
   #
   ```
4. Enter the following command to enable CONFIG mode:
   ```
   configure terminal
   ```
5. Enter the following command to configure software autoupgrade:
   ```
   software autoupgrade <urlstring> [username] [password]
   ```
   where
   - **upgrade URL string** is the location where the upgradeConfig.json file is hosted.
   - **username** and **password** are credentials to access the upgradeConfig.json file.
6. Enter the following command to exit:
   ```
   end
   ```

Related topics

- "Disabling auto-upgrade" on the next page
- "Viewing auto-upgrade details" below

Viewing auto-upgrade details

Do the following to view the auto-upgrade configuration details.

Procedure

1. Log into the Standalone Sentry command line interface (CLI) using the administrator account you created during installation.
2. Enter the following command to switch to EXEC Privileged mode:
   ```
   enable
   ```
3. Enter the password for enabling the EXEC Privileged mode.
The command line prompt changes:
#
4. Enter the following command to view auto-upgrade configuration:
   show software autoupgrade
   The auto-upgrade configuration details are displayed.
5. Enter the following command to exit:
   end

Disabling auto-upgrade

When auto-upgrade is enabled, Standalone Sentry checks for upgrades every thirty minutes. Do the following to disable auto-upgrade.

Procedure
1. Login to the CLI using the administrator account you created during installation.
2. Enter the following command to switch to EXEC Privileged mode:
   enable
3. Enter the password for enabling the EXEC Privileged mode.
   The command line prompt changes:
   #
4. Enter the following command to enable CONFIG mode:
   configure terminal
5. Enter the following command to disable auto-upgrade:
   no software autoupgrade
   The auto-upgrade configuration details are removed.
6. Enter the following command to exit:
   end