Sentry 9.14.0 - 10.0.0 Guide for Ivanti EPMM

June 2024

Copyright © 2024, Ivanti, Inc. All rights reserved.
Privacy and Legal

Contents

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
June 28, 2024	Updated for 9.14.0 - 10.0.0 Ivanti Standalone Sentry.
March 28, 2024	Updated for 9.14.0 - 9.20.0 Ivanti Standalone Sentry.
October 23, 2023	Updated for 9.14.0 - 9.19.0 Ivanti Standalone Sentry.
July 18, 2023	Updated for 9.14.0 - 9.18.0 Ivanti Standalone Sentry.
May 29, 2023	Updated "OAuth for Sentry on Ivanti EPMM" on page 69.
January 10, 2023	Updated "Multi-factor authentication configuration for Ivanti EPMM" on page 76 for Android and iOS Email+ configuration.
December 15, 2022	Updated for 9.14.0 - 9.17.0 Sentry.
September 26, 2022	Updated "Checking TLS compliance" on page 306 with disabled TLS versions.
August 08, 2022	Updated for 9.16.0 Sentry.
April 05, 2022	Updated for 9.14.0 - 9.15.0 Sentry.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

About Sentry

The following provide information about Sentry:

Ivanti Standalone Sentry overview

Ivanti Standalone Sentry is a part of 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 - Ivanti EPMM or Ivanti Neurons for MDM.

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. An Access deployment requires a unified endpoint management (UEM) platform, Ivanti Standalone Sentry, and Ivanti 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" on the next page
  - "Sentry and UEM platform support" on the next page
  - "Integrated Sentry" on the next page
  - "ActiveSync with Ivanti Standalone Sentry" on page 9
  - "AppTunnel with Ivanti Standalone Sentry" on page 10
  - "Network traffic support with AppTunnel" on page 10
  - "Ivanti Standalone Sentry as a KKDCP server (Ivanti EPMM only)" on page 11

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Sentry flavors

Sentry is available in two flavors: Ivanti Standalone Sentry or Integrated Sentry.

Ivanti Standalone Sentry is a separate appliance that acts as a gateway between devices and your ActiveSync-enabled email servers or backend resource. Ivanti Standalone Sentry can be configured for ActiveSync or AppTunnel, or as Kerberos Key Distribution Center Proxy (KKDCP) server. Ivanti Standalone Sentry can be installed on premise on a Appliance or a virtual appliance. Or, Ivanti 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.

Ivanti Standalone Sentry gets input from the unified endpoint management (UEM) platform, Ivanti EPMM or Ivanti Neurons for MDM, to do the following:

- Integrated Sentry or the Ivanti Standalone Sentry configured for ActiveSync protects the ActiveSync server from wrongful access from devices.
- Ivanti 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 2. SENTRY AND UEM PLATFORM SUPPORT

Sentry	UEM platform
Integrated Sentry	Ivanti EPMM
Ivanti Standalone Sentry (on-premise, AWS, and Microsoft Azure)	Ivanti EPMM, Ivanti Neurons for MDM

Integrated Sentry

Integrated Sentry is a policy agent for Microsoft Exchange Server email clusters, and for Microsoft Office 365. It is packaged as a software module on the Exchange Server or on a separate server with Exchange Server access.

Integrated Sentry passes information between Ivanti EPMM and Microsoft Exchange Server. For example:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Ivanti EPMM periodically syncs with Integrated Sentry to get the list of ActiveSync devices. Integrated Sentry gets the list from the Exchange Server.
- Ivanti EPMM informs Integrated Sentry when an ActiveSync device is in violation of its security policy. Integrated Sentry tells the Exchange Server to block the device.
- Ivanti EPMM informs Integrated Sentry when too many ActiveSync devices have the same mailbox. Integrated Sentry tells the Exchange Server to block the device.
- Ivanti EPMM informs Integrated Sentry when the Ivanti EPMM administrator blocks, allows, or wipes an ActiveSync device in the Ivanti EPMM Admin Portal. Integrated Sentry tells the Exchange server to take the appropriate action.
- Ivanti EPMM passes an ActiveSync policy to Integrated Sentry. You configure the policy using the Admin Portal. Integrated Sentry passes the policy to the Exchange Server, which updates its own policy, and passes the policy to the device.

Ivanti strongly recommends deploying Ivanti Standalone Sentry if you are supporting more than 5000 devices with Office 365.

ActiveSync with Ivanti Standalone Sentry

Ivanti 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 "Ivanti EPMM, Ivanti Standalone Sentry, and device interaction" on page 15.

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***. Ivanti Standalone Sentry and the UEM platform work together to protect the ActiveSync server from wrongful access by these devices.

Communication between Ivanti Standalone Sentry and ActiveSync servers is encrypted using HTTPS. Administrators can enable server TLS and configure outbound SSL. For Office 365 and GMail, Ivanti, Inc 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

AppTunnel with Ivanti Standalone Sentry

Ivanti 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 an Ivanti Tunnel deployment. However, AppTunnel is not a requirement for an AppConnect app deployment.

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

- UEM provides Ivanti Standalone Sentry with the backend resource configuration for the app.
- When an app attempts to connect to a backend resource, Ivanti Standalone Sentry creates an app tunnel which is a unique combination of user, device, and app. Ivanti Standalone Sentry provides information about the app tunnel to the UEM.
- UEM informs Ivanti Standalone Sentry when an app should not be allowed to access the backend resource. For example, Ivanti 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 3. SUPPORTED NETWORK TRAFFIC FOR APPTUNNEL

Protocol	Support
HTTP, HTTPS tunneling	• Android and iOS AppConnect apps
TCP tunneling	• Android AppConnect apps • iOS and macOS managed apps with Tunnel configured for app proxy VPN. • Web@Work with Chromium stack enabled. TCP tunnels support HTTP and HTTPS traffic also.
IP tunneling	• Windows 10, iOS, and Android managed apps with Ivanti Tunnel. IP tunnels also support HTTP, HTTPS, TCP, and UDP traffic.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry as a KKDCP server (Ivanti EPMM only)

Standalone Sentry can be configured as a Kerberos Key Distribution Center Proxy (KKDCP) server. A separate Standalone Sentry is required for Kerberos proxy. Standalone Sentry as a KKDCP server is only supported with Ivanti EPMM.

Benefits of Ivanti Standalone Sentry

Benefits of using Sentry in your deployment include the following:

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

Device and user authentication support with Ivanti Standalone Sentry

Using Ivanti 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 Ivanti Standalone 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. Ivanti Standalone Sentry gets device posture and compliance information from UEM, and allows access based on the device posture.

ActiveSync policy and Sentry (Ivanti EPMM only)

When you use Sentry for ActiveSync, you also have the option to configure an ActiveSync policy that is applied to the device. The ActiveSync policy determines, for example, the password requirements for devices, whether you require device encryption, and whether devices can access email using a browser.

An ActiveSync device is typically registered. However, for devices that cannot support the Ivanti EPMM-provided policies, you can use the ActiveSync policy to support your organization’s security requirements.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Visibility into which devices are accessing the backend resource with Sentry

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

Ivanti Standalone Sentry for ActiveSync creates a unique record for each combination of user and device accessing the ActiveSync server. Ivanti 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.

Ivanti Standalone Sentry for AppTunnel creates a unique AppTunnel session (connection) for each unique combination of user, app, and device. For example, Ivanti 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.

Integrated Sentry gets the list of ActiveSync devices and users from the Microsoft Exchange Server, and provides the list to Ivanti EPMM. From the Admin Portal, you can then control every device that accesses the ActiveSync server, regardless of whether the device is registered with Ivanti EPMM.

Ability to take action on ActiveSync device with Sentry

Ivanti EPMM

You can take actions on ActiveSync devices. For example, you can block email access on a device, or wipe the device (reset it to factory defaults). You can take these actions regardless of whether an ActiveSync device is registered with Ivanti EPMM.

You can also take action on AppTunnels. You can Allow or Block an AppConnect app on a device from accessing the backend resource. You can also Remove an AppTunnel.

Ivanti Standalone Sentry deployment scenarios

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

These deployments include:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- "Deployment with Ivanti Standalone Sentry in the DMZ" below
- "Deployment with multiple Ivanti Standalone Sentry servers" below
- "Deployment with Ivanti Standalone Sentry behind a proxy" on the next page
- "Deployment with multiple ActiveSync servers or backend resources" on page 15

Deployment with Ivanti Standalone Sentry in the DMZ

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

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

Deployment with multiple Ivanti Standalone Sentry servers

Use multiple Ivanti Standalone Sentrys in the following situations:

- Ivanti Standalone Sentry and Integrated Sentry for High Availability

  Multiple Standalone Sentrys and Integrated Sentrys can back each other up to provide High Availability access to ActiveSync Servers or backend resources. In this configuration, each Sentry points to the same server or server cluster. Contact Professional Services to set up this configuration.

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

  An Ivanti 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 Sentrys. 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*.

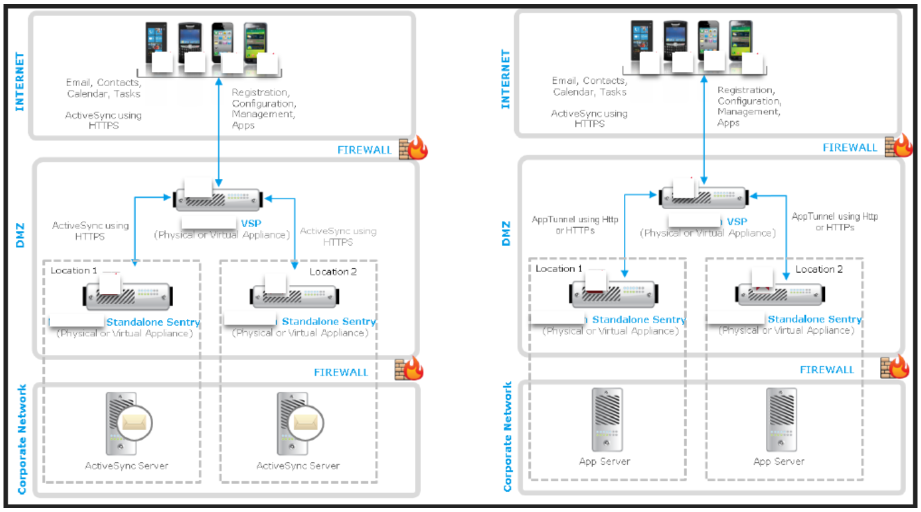
- You have multiple ActiveSync or backend resources, each of which supports a different organization.

  Use one Ivanti Standalone Sentry for each organization. Configure the Ivanti 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 an Ivanti 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 1. SENTRY IN DIFFERENT LOCATIONS


INTERNET
Email, Contacts, Calendar, Tasks
ActiveSync using HTTPS
Registration, Configuration, Management, Apps
FIREWALL
DMZ
ActiveSync using HTTPS
VSP
(Physical or Virtual Appliance)
ActiveSync using HTTPS
Location 1
Location 2
Standalone Sentry
(Physical or Virtual Appliance)
Standalone Sentry
(Physical or Virtual Appliance)
FIREWALL
Corporate Network
ActiveSync Server
ActiveSync Server
INTERNET
Email, Contacts, Calendar, Tasks
ActiveSync using HTTPS
Registration, Configuration, Management, Apps
FIREWALL
DMZ
AppTunnel using Http or HTTPs
VSP
(Physical or Virtual Appliance)
AppTunnel using Http or HTTPs
Location 1
Location 2
Standalone Sentry
(Physical or Virtual Appliance)
Standalone Sentry
(Physical or Virtual Appliance)
FIREWALL
Corporate Network
App Server
App Server

Typically, you use load balancers when using multiple Standalone Sentrys. 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 Ivanti Standalone Sentry behind a proxy

You can configure the Ivanti 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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Setting up an Apache or F5 proxy to front-end the Ivanti 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 Ivanti 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 Ivanti Standalone Sentry and the active ActiveSync servers or backend resource.

Ivanti EPMM, Ivanti Standalone Sentry, and device interaction

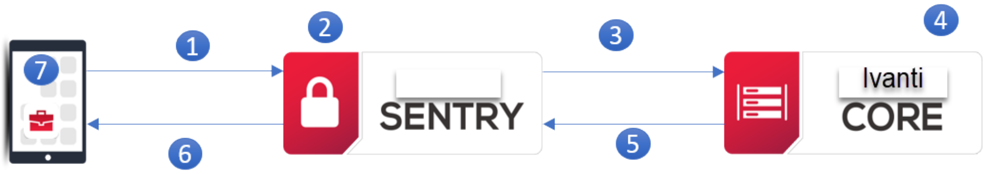
The following describe Ivanti EPMM, Ivanti Standalone Sentry, and device interaction:

- "When an ActiveSync device accesses email" below
- "When an app accesses the backend resource" on the next page
- "When Ivanti EPMM detects a security policy violation" on page 17
- "When you change an ActiveSync policy (Ivanti EPMM only)" on page 17
- "When Sentry initializes" on page 17
- "Periodic Ivanti EPMM-Standalone Sentry resync" on page 18

When an ActiveSync device accesses email

The following illustrates the interaction between Ivanti 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



Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

1. Device attempts to access ActiveSync or other backend resource.
2. Ivanti Standalone Sentry adds device to its list of devices.
3. Ivanti Standalone Sentry tells UEM about the device.
4. The ActiveSync devices view on the UEM now includes the device.
5. UEM tells Ivanti Standalone Sentry whether to block or allow the device based on:
   - the device's security policy
   - whether the maximum number of devices per mailbox has been exceeded
   - whether you specified to auto block unregistered devices
6. Ivanti Sentry tells device whether it is blocked or allowed, passing ActiveSync policy if allowed.
7. If access is allowed, device applies ActiveSync policy, and continues email processing.
   If access is blocked, Standalone Sentry informs the device.

The next time a device attempts to access the ActiveSync server, the device is already in the list of devices on Standalone Sentry. Therefore, Ivanti Standalone Sentry already has the information in the UEM about whether to block or allow access.

If Ivanti Standalone Sentry cannot communicate with UEM

On the first attempt, if Ivanti Standalone Sentry is temporarily unable to communicate with UEM due to, for example, a network error, the following occurs:

1. Ivanti Standalone Sentry allows the device to access the ActiveSync server.
2. Ivanti Standalone Sentry pushes a default ActiveSync policy to the device.
   This default policy is not the same as the default ActiveSync policy you configure in the Admin Portal. This default policy is a temporary policy to cover this infrequent communication failure.
3. At a periodic UEM-Sentry resync, the UEM sends Ivanti Standalone Sentry the proper state of the device (allowed, blocked, or wiped) as well as the device's ActiveSync policy. If access is allowed, Standalone Sentry pushes the ActiveSync policy to the device.

When an app accesses the backend resource

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

1. UEM tells Ivanti Standalone Sentry whether to allow or block the app’s access to the backend resource based on:
    - the device’s security policy
    - whether you specified to auto block unregistered devices
    - whether the app is an authorized app
2. Ivanti 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. Ivanti Standalone Sentry allows the app to access the backend resource.
2. At the periodic Ivanti EPMM-Sentry resync, the UEM sends Ivanti Standalone Sentry the proper state of the device (allowed, blocked, or wiped).

When Ivanti EPMM detects a security policy violation

UEM detects a security policy violation when, for example, a device checks in. UEM tells Standalone Sentry to block the device from accessing the ActiveSync server and backend resources.

When you change an ActiveSync policy (Ivanti EPMM only)

On the Admin Portal, you can add or modify ActiveSync policies. For each affected device, Ivanti EPMM sends the ActiveSync policy to Standalone Sentry. Standalone Sentry sends the policy to the device.

When Sentry initializes

When Ivanti Standalone Sentry starts or restarts, the following occurs:

1. Ivanti Standalone Sentry gets all the registered ActiveSync devices from UEM that are allowed to access the ActiveSync server.
2. Ivanti Standalone Sentry puts all these devices in its list of devices. The information in the list includes the ActiveSync policy for each device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Creating this list speeds up the time it takes for devices to access their email after a Sentry maintenance restart, especially when Ivanti EPMM and Ivanti Standalone Sentry communicate over a high latency link. The performance improvement is because the Standalone Sentry does not have to ask Ivanti EPMM whether to block or allow most devices' access to the ActiveSync server.
If a device is not in the list, the device's next attempt to access the ActiveSync server is as though it is the first time. See "When an ActiveSync device accesses email" on page 15.

3. Ivanti Standalone Sentry retrieves the AppTunnels equal to the Sentry device cache size (number).

Periodic Ivanti EPMM-Standalone Sentry resync

Sometimes communication errors can occur between the following:

- Ivanti EPMM and Ivanti Standalone Sentry

  A communication error can occur because of a network problem. For example

  These communication errors can result in UEM failing to tell Ivanti Standalone Sentry to block, allow, or wipe a device, or failing to send Standalone Sentry an updated or new ActiveSync policy, or failing to tell Ivanti Standalone Sentry to block, allow, or remove an AppTunnel.

- Ivanti Standalone Sentry and a device

  For example, a device can be turned off when you update its ActiveSync policy.

Therefore, Ivanti EPMM and Sentry periodically resync to make sure that they and the ActiveSync devices have the correct data. For example, Standalone Sentry updates its list of devices with the proper state of each ActiveSync device (allowed, blocked, or wiped), the ActiveSync policy if it changed, the state for each AppTunnel (allowed, blocked, or removed). Ivanti Standalone Sentry also pushes updated ActiveSync policies to the devices.

Persistent device list

Ivanti 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.

Ivanti Standalone Sentry also uses a persistent device list, sometimes known as a persistent cache. Ivanti Standalone Sentry persists on disk, which means stores on disk, its list of ActiveSync devices. When Ivanti Standalone Sentry initializes, if it cannot reach UEM due to, for example, network issues, it uses its persistent device list to begin its operations. In this way, Ivanti Standalone Sentry can begin with the last known state of each of its ActiveSync devices.

Ivanti Standalone Sentry updates the persistent device list as follows:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- At regular intervals. This update to disk is called the *periodic disk update*.
- Before shutting down.
- When requested by a CLI command.

Ivanti Standalone Sentry behavior when UEM is not reachable

Now, when Ivanti Standalone Sentry detects that it cannot reach Ivanti EPMM, it reacts depending on the following situations:

- Ivanti Standalone Sentry is initializing but cannot reach Ivanti EPMM to get the list of devices.

  Normally, when it initializes, Ivanti Standalone Sentry retrieves from Ivanti EPMM all the registered ActiveSync devices that are allowed to access the ActiveSync server. If Ivanti EPMM is not reachable, Standalone Sentry reads into memory the persistent device list that it last stored on disk. Therefore, Ivanti Standalone Sentry continues operating using the last known state of each device.
  To understand Standalone Sentry initialization behavior when it *can* reach Ivanti EPMM, see "Ivanti EPMM, Ivanti Standalone Sentry, and device interaction" on page 15.

- At some point after initialization is complete, Ivanti Standalone Sentry cannot reach Ivanti EPMM after trying for an internally specified time period.

  In this situation, Ivanti Standalone Sentry continues operating using the last known state of the device as stored in its in-memory list.

- If Ivanti EPMM is unreachable, and a new device or device not in the Ivanti Standalone Sentry persistent device list, accesses the ActiveSync server or backend resource, the default Sentry behavior allows access to the server. In this case, for ActiveSync traffic, the ActiveSync server's policy is applied to the new device.

Although Ivanti Standalone Sentry continues operating, being unable to reach Ivanti EPMM has the following impact:

- The Ivanti Standalone Sentry does not know when Ivanti EPMM changes the state of a device due to a security policy violation.
- It does not know when you change the state of the device using the ActiveSync Devices view of the Admin Portal.
- It does not know when you change the ActiveSync policy for a device using the Admin Portal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- It cannot get guidance from Ivanti EPMM when a device that is not in its list attempts to access the ActiveSync server. This situation occurs, for example, when a new device has registered with Ivanti EPMM. Ivanti Standalone Sentry allows the device access to the ActiveSync server and pushes a default ActiveSync policy to the device.

Ivanti Standalone Sentry behavior when UEM is reachable again

Ivanti Standalone Sentry detects when Ivanti EPMM becomes reachable. The Standalone Sentry does the following:

- Retrieves all the registered ActiveSync devices from Ivanti EPMM that are allowed to access the ActiveSync server, and updates its in-memory device list with them.

- Resumes normal interactions with Ivanti EPMM as described in "Ivanti EPMM, Ivanti Standalone Sentry, and device interaction" on page 15.

Checking if Ivanti Standalone Sentry can reach UEM

You can check whether Ivanti Standalone Sentry can reach UEM by using the Ivanti Standalone Sentry System Manager. See "Service Diagnosis" on page 259.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

Ivanti Standalone Sentry features for Ivanti EPMM

- **Support for Oracle Linux 8**: The Ivanti Standalone Sentry platform is now upgraded from CentOS7 to Oracle Linux 8.
- **Sentry self-signed certificate warning**: Ivanti Standalone Sentry displays a warning message when customers attempt to generate and use a self-signed certificate for a TLS handshake between Sentry and Tunnel. For more information, see Configuring Ivanti Standalone Sentry for AppTunnel.

Related information from previous releases

If a release does not appear in this section, then there were no associated new features and enhancements.

- Ivanti Standalone Sentry 9.20.0 - New features summary
- Ivanti Standalone Sentry 9.18.0 - New features summary
- Ivanti Standalone Sentry 9.17.0 - New features summary
- Ivanti Standalone Sentry 9.16.0 - New features summary
- Ivanti Standalone Sentry 9.15.0 - New features summary
- Ivanti Standalone Sentry 9.14.0 - New features summary

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry Configuration Overview

The initial setup of Sentry is done as part of the installation process. Additional Sentry configuration for ActiveSync, AppTunnel, KKDCP, certificates, and Sentry preferences is done on the Ivanti EPMM Admin Portal. These settings specify how Sentry connects to Ivanti EPMM, the ActiveSync server, backend resources, and to devices. Ivanti Standalone Sentry system management occurs on the Ivanti Standalone Sentry System Manager.

Ivanti Standalone Sentry Initial setup

For information about initial setup, see the following:

- If you are using an on-premise Ivanti EPMM, see the On-Premise Installation Guide.

Before continuing with Sentry configuration using the Ivanti EPMM Admin Portal, ensure that you have installed Ivanti Standalone Sentry.

Ivanti Standalone Sentry configurations on Ivanti EPMM

- Integrated Sentry configuration

See "Working with Integrated Sentry" on page 27

- Ivanti Standalone Sentry configuration

See "Ivanti Standalone Sentry for ActiveSync Email" on page 39
See "Ivanti Standalone Sentry for AppTunnel" on page 93
See Ivanti Standalone Sentry for KKDCP

- Certificates configuration

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

See "Device and Server Authentication" on page 109
See "Ivanti Standalone Sentry certificate" on page 148

- ActiveSync policy configuration

See "ActiveSync Policies" on page 129

- Sentry preferences configuration

See "Sentry preferences" on page 144

Configurations in Ivanti Standalone Sentry System Manager

Settings in the System Manager include Ivanti 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:

- "Ivanti Standalone Sentry Settings" on page 175
- "Ivanti Standalone Sentry Security Settings" on page 229
- "Ivanti Standalone Sentry Maintenance Settings" on page 245
- "Troubleshooting" on page 251
- "Monitoring" on page 265

Related topics
"Accessing the Ivanti Standalone Sentry System Manager" on the next page.

Integrated Sentry and Ivanti Standalone Sentry on the same Ivanti EPMM

Both Ivanti Standalone Sentry with Microsoft Exchange and Integrated Sentry with Microsoft Office 365 can be configured on the same Ivanti EPMM. You may want to configure both Ivanti Standalone Sentry and Integrated Sentry on the same Ivanti you are migrating from one to the other.

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Accessing the Ivanti Standalone Sentry System Manager

Ivanti recommends allowing HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for Ivanti Standalone Sentry System Manager and must have strictly controlled access. The following provides the steps to access the Ivanti Standalone System manager.

Procedure

1. Enter the following URL in browser:

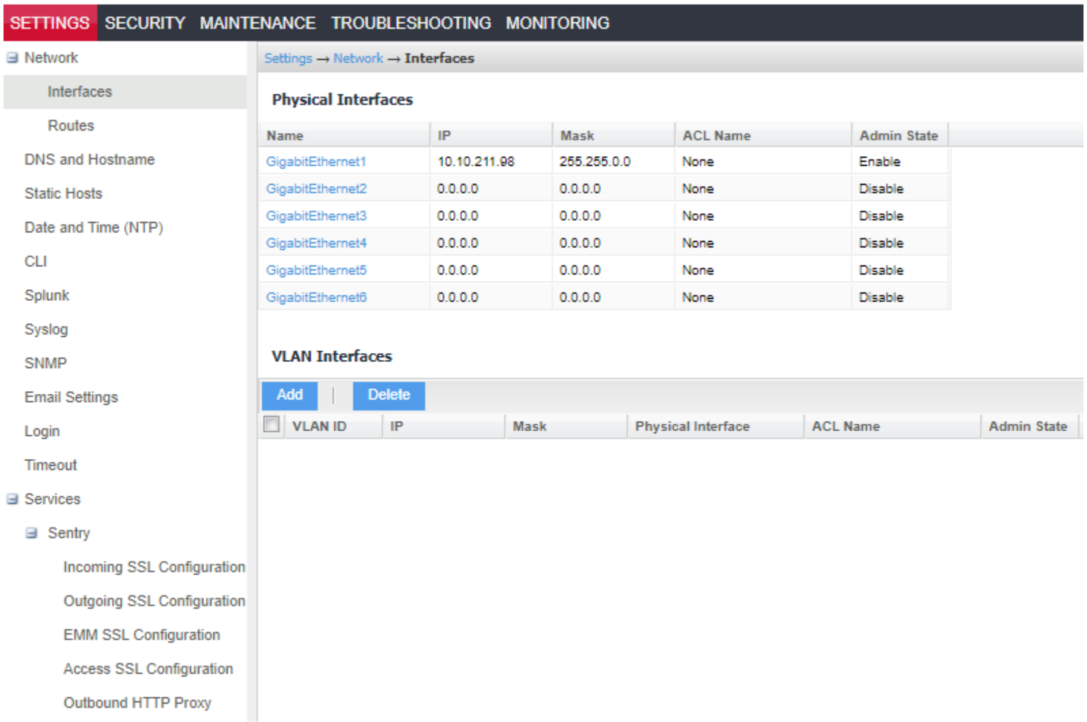
https://<*fully_qualified_hostname*>:8443

The version number will change depending on the version of the Ivanti Standalone Sentry.

2. Enter a user ID and password for the Ivanti 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 1. IVANTI STANDALONE SENTRY SYSTEM MANAGER



Physical Interfaces

Name	IP	Mask	ACL Name	Admin State
GigabitEthernet1	10.10.211.98	255.255.0.0	None	Enable
GigabitEthernet2	0.0.0.0	0.0.0.0	None	Disable
GigabitEthernet3	0.0.0.0	0.0.0.0	None	Disable
GigabitEthernet4	0.0.0.0	0.0.0.0	None	Disable
GigabitEthernet5	0.0.0.0	0.0.0.0	None	Disable
GigabitEthernet6	0.0.0.0	0.0.0.0	None	Disable

VLAN Interfaces

□	VLAN ID	IP	Mask	Physical Interface	ACL Name	Admin State

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Working with Integrated Sentry

The following describe how to configure Integrated Sentry on Ivanti EPMM:

Before you configure Integrated Sentry

You must have installed Integrated Sentry. See the *Integrated Sentry Installation and Upgrade Guide*.

Integrated Sentry configuration overview

Integrated Sentry is a Windows service that interacts with the Microsoft Exchange Server. After you finish installing the service, in the Admin Portal, go to **Services > Sentry** to configure Integrated Sentry settings. These settings specify how Integrated Sentry connects to Ivanti EPMM, the ActiveSync server, and to devices.

These settings include:

- The host name or IP addresses of the Integrated Sentry and an alternate Integrated Sentry.
- The port on Integrated Sentry and alternate Integrated Sentry that Ivanti EPMM uses to access Sentry.
- The password that Ivanti EPMM uses to connect to Integrated Sentry.
- The LDAP groups that you control with Integrated Sentry.
- Information necessary when using a hosted Exchange server (Microsoft Office 365).

The following sections describe Integrated Sentry related configurations in the Admin Portal:

- Integrated Sentry connectivity.

See "Adding an entry for Integrated Sentry in Ivanti EPMM" on the next page.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Sync Integrated Sentry with Exchange.

See "Sync Integrated Sentry with Exchange " on page 35.

- Edit a Sentry entry.

See "Editing, deleting, disabling, and enabling a Sentry entry in Ivanti EPMM" on page 141.

- Sentry preferences.

See "Sentry preferences" on page 144.

- Manage ActiveSync associations.

See "Managing ActiveSync Email Devices" on page 153.

Adding an entry for Integrated Sentry in Ivanti EPMM

Create an entry for a Integrated Sentry on Ivanti EPMM to specify how Integrated Sentry connects to Ivanti EPMM, the ActiveSync server, and to devices.

- "Configuring Integrated Sentry on Ivanti EPMM: Exchange 2010" below
- "Configuring Integrated Sentry on Ivanti EPMM: Hosted Exchange (Office 365)" on page 30

Additional configuration for Integrated Sentry hosted on Office 365:

- "Specifying Office 365 groups for sync (optional)" on page 32

Configuring Integrated Sentry on Ivanti EPMM: Exchange 2010

Follow the configuration described here if you have installed Integrated Sentry on Exchange 2010.

Procedure

1. Login to the Admin Portal with a user account that has at least the Settings role and Users & Devices role.
2. Go to **Services > Sentry**.
3. Select **Add New > Integrated Sentry**.
4. Use the guidelines in the following table to configure the Integrated Sentry:

Item	Description
Server	Specify the IP address or host name for the server on which you installed Integrated Sentry.

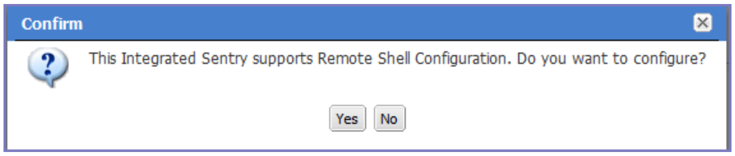
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Item	Description
Port	Specify the port to use to connect to the server on which you installed Integrated Sentry.
Secondary Server	Specify the IP address or host name for an alternate server on which you installed Integrated Sentry. Ivanti EPMM uses this secondary Integrated Sentry if the primary one is not available. ⓘ Your secondary Integrated Sentry must be installed with the same Microsoft Exchange option as your primary Integrated Sentry. For example, if you use Microsoft Exchange Server 2010, you have to select Microsoft Exchange 2010 in the Integrated Sentry installer when installing both the primary Integrated Sentry and the secondary Integrated Sentry.
Secondary Port	Specify the port to use to connect to the alternate server on which you installed Integrated Sentry.
Secret	Specify the password for connecting to the Integrated Sentry server. This value is the same as the connection secret you entered when running the Integrated Sentry installer.
Confirm Secret	Re-enter the password for connecting to the Integrated Sentry server.
Search LDAP Groups	Enter the name of an LDAP group, or the first few letters of an LDAP group name, and then select the search icon to the right of the text field. Matching groups appear in the Available list in the Apply To LDAP Groups field. Use this field when you intend to use more than one Integrated Sentry, where each one handles a subset of all possible LDAP groups. This field allows you to select the LDAP groups that this Integrated Sentry handles.
Apply to LDAP Groups	After you have selected the LDAP groups to select from, move groups from the Available list to the Selected list. If you put no groups in the Selected list, the Integrated Sentry handles all the LDAP groups.

5. Click **Save**.

If the machine on which you installed Integrated Sentry has both Exchange Management Tools and PowerShell 2.0 installed, the following pop-up appears:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.


Confirm

This Integrated Sentry supports Remote Shell Configuration. Do you want to configure?

Click **No**.

6. Click **Resync Integrated Sentry With Exchange**.
7. Select **Users & Devices > ActiveSync Associations**.
8. If an error appears before the page begins to populate, navigate away from the page and then back. You should see your ActiveSync users begin to populate.

It may take up to 15 minutes to populate all users in this screen.

Configuring Integrated Sentry on Ivanti EPMM: Hosted Exchange (Office 365)

Follow the configuration described here if you have installed Integrated Sentry on Office 365.

Procedure

1. Login to the Admin Portal using a user account that has at least the Settings role and Users & Devices role.
2. Select **Services > Sentry**.
3. Select **Add New > Integrated Sentry**.
4. Use the guidelines in the following table to configure the Integrated Sentry:

Item	Description
Server	Specify the IP address or host name for the server on which you installed Integrated Sentry.
Port	Specify the port to use to connect to the server on which you installed Integrated Sentry.
Secondary Server	Specify the IP address or host name for an alternate server on which you installed Integrated Sentry. Ivanti EPMM uses this secondary Integrated Sentry if the primary one is not available. ⓘ Both your primary and secondary Integrated Sentry must be installed with the “hosted exchange” option in the Integrated Sentry installer.
Secondary Port	Specify the port to use to connect to the alternate server on which you installed Integrated Sentry.

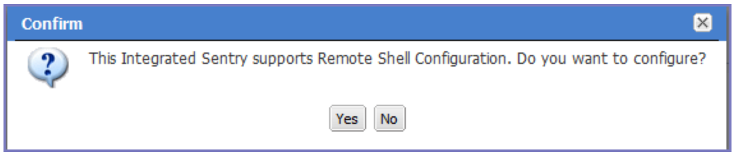
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Item	Description
Secret	Specify the password for connecting to the Integrated Sentry server. This value is the same as the connection secret you entered when running the Integrated Sentry installer.
Confirm Secret	Re-enter the password for connecting to the Integrated Sentry server.
Search LDAP Groups	This field is not applicable when using a hosted Exchange server. Do not use this field.
Apply to LDAP Groups	This field is not applicable when using a hosted Exchange server. Do not use this field.

5. Click **Save**.

If the machine on which you installed Integrated Sentry has PowerShell 2.0 installed, but not Exchange Management Tools, an additional section automatically displays when you click Save.

However, if the machine on which you installed Integrated Sentry has Exchange Management Tools installed, the following pop-up appears:



This Integrated Sentry supports Remote Shell Configuration. Do you want to configure?

Click **Yes**.

6. Use the following guidelines to complete the lower portion of the screen:

Option	Description
Remote Exchange FQDN	Enter the fully-qualified domain name for the hosted Exchange server as supplied by Microsoft. For Office 365, this value is ps.outlook.com.
Authentication	Select Basic for Office 365.
Use SSL	We recommend using SSL for the connection between Integrated Sentry and the hosted Exchange server. If you do not use SSL, take the steps specified in “SSL and Hosted Exchange” in the On-Premise Installation Guide.
Skip server CA checks	This field is not applicable to Office 365.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Option	Description
Use service credentials	Do not select this option when using Office 365. Clear this option to specify separate credentials for this connection. Specify the separate credentials in the User Name and Password fields below this option.
User Name	Enter the user name to use for this connection if you are not using the service credentials. Note that the user name typically includes the domain name, such as domain_name\username.
Password	Enter the password to use for the connection if you are not using the service credentials.
Confirm Password	Re-enter the password.
Don’t save credentials on Ivanti EPMM	Select this option if the credentials you entered in the User Name and Password fields should not be stored on Ivanti EPMM. Credentials are encrypted when stored Ivanti EPMM, but some organizations may prefer not to have credentials for hosted systems stored on external systems.

7. Click **Save**.
8. Click **Resync Integrated Sentry with Exchange**.
9. Select **Users & Device > Devices**.
10. If an error appears before the page begins to populate, navigate away from the page and then back. You should see your ActiveSync users begin to populate.

It may take up to 15 minutes to populate all users in this screen.

Next steps

Go to "Specifying Office 365 groups for sync (optional)" below.

Specifying Office 365 groups for sync (optional)

Use the configuration described here only if you have installed Integrated Sentry on Office 365.

You cannot specify Office 365 groups to sync for dedicated Office 365 deployments.

Setting up Office 365 groups to sync is optional. If a group is not configured, then Integrated Sentry syncs all mailboxes in Office 365.

Setting up syncing for specific Office 365 groups provides the following benefits:

- Allows administrators to enforce Integrated Sentry access control to specific groups in Office 365.

  You may want to do this if you only want mailboxes in certain groups to be managed through Integrated Sentry.

- Targeting specific Office 365 groups for sync allows Integrated Sentry to complete sync faster.

ⓘ Security policies and access control is only applied to mailboxes that are synced with Integrated Sentry.

Before you begin

Ensure you have the Office 365 Group IDs for syncing. To find the full names of the desired group, run the following PowerShell command in a connected remote PowerShell session to Office 365:

```
Get-Group | Select-Object Name, DistinguishedName | fl
```

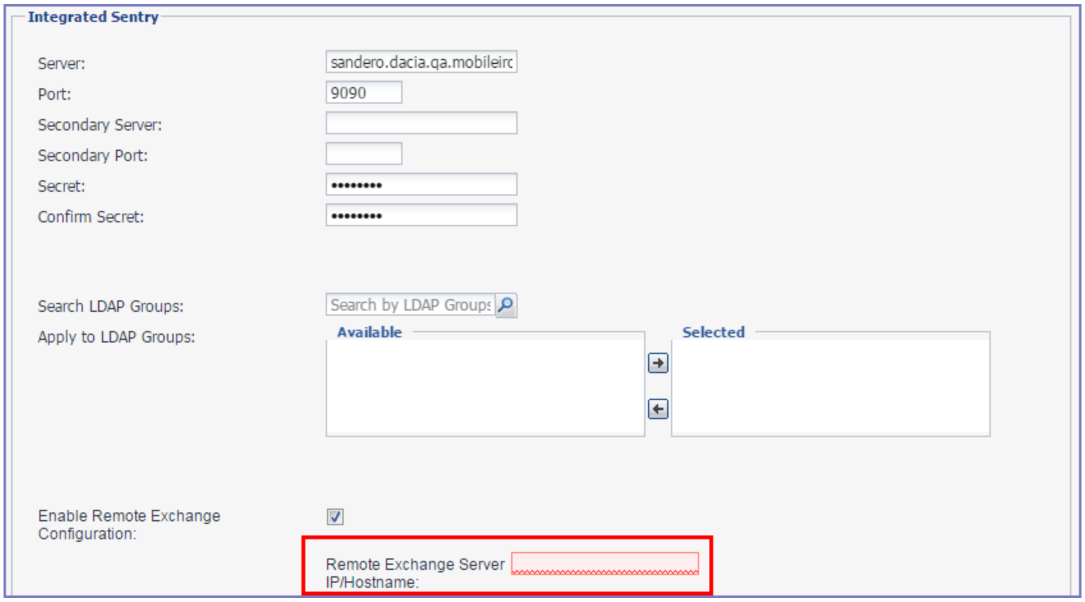
Procedure

1. In Ivanti EPMM Admin Portal, go to **Services > Sentry**.
2. Click on the **Edit** icon for the Integrated Sentry.

The **Edit Integrated Sentry** window appears.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. EDIT INTEGRATED SENTRY



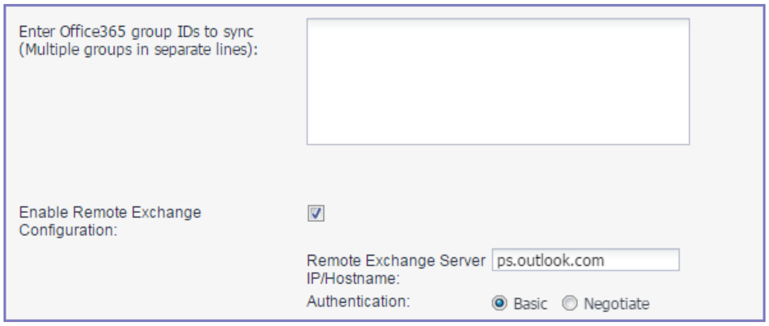
Integrated Sentry

Server:	sandero.dacia.qa.mobileirc
Port:	9090
Secondary Server:	
Secondary Port:	
Secret:	••••••••
Confirm Secret:	••••••••
Search LDAP Groups:	Search by LDAP Groups
Apply to LDAP Groups:	Available / Selected
Enable Remote Exchange Configuration:	☑
Remote Exchange Server IP/Hostname:	

3. For **Remote Exchange Server IP/Hostname**, enter *ps.outlook.com*.

The **Search LDAP Groups** and **Apply to LDAP** Groups fields are replaced with the **Enter Office 365 group IDs to sync** field.

FIGURE 2. ENTER OFFICE 365 GROUP IDS



Enter Office365 group IDs to sync (Multiple groups in separate lines):	
Enable Remote Exchange Configuration:	☑
Remote Exchange Server IP/Hostname:	ps.outlook.com
Authentication:	● Basic ○ Negotiate

4. In the **Enter Office 365 group IDs to sync** text box, enter the Office 365 group IDs.

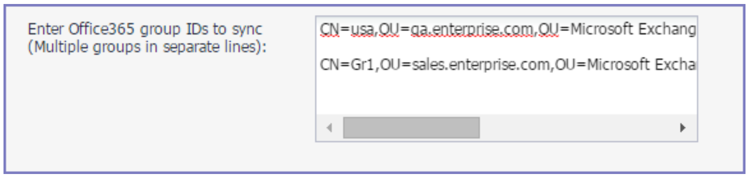
If you are entering multiple Office 365 groups, list each group ID in a separate line.

Enter the full Distinguished Name of the groups in O365.

Example: CN=usa,OU=qa.enterprise.com,OU=Microsoft Exchange Hosted organizations,DC=NAMPR06A003,DC=prod,DC=outlook,DC=com

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 3. EXAMPLE FOR MULTIPLE OFFICE 365 GROUPS



Enter Office365 group IDs to sync (Multiple groups in separate lines):

CN=usa,OU=qa.enterprise.com,OU=Microsoft Exchang
CN=Gr1,OU=sales.enterprise.com,OU=Microsoft Excha

5. Click **Save**.

Sync Integrated Sentry with Exchange

After the initial set up, Integrated Sentry automatically performs a full mailbox sync with the Exchange server. It attempts to sync the entire list of mailboxes on the Exchange server. Since a full mailbox sync can cause sync failures in a large setup, initially, Integrated Sentry performs a batched sync. Subsequently, Integrated Sentry performs a periodic differential sync.

- "Batched sync of mailboxes " below
- "Periodic differential sync" on the next page
- "Manually resyncing Integrated Sentry with Exchange" on the next page

Batched sync of mailboxes

Starting with version 6.1, Integrated Sentry performs a full sync of the entire list of mailboxes and devices in batches. In case of a failure, the sync restarts where it had stopped. This reduces the time needed for a full sync, and it removes the need to re-do the entire sync operation.

Integrated Sentry automatically performs a full batched resync of all mailboxes and devices:

- once every seven days. The next full resync is calculated based on the last successful full resync.
- if a periodic differential sync is unsuccessful.
- if there are changes in Exchange settings that might impact a large number of devices.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Periodic differential sync

After a full sync, Integrated Sentry performs periodic differential syncs. At regular intervals, Integrated Sentry checks for any changes in devices or mailboxes and only updates the changes since the last successful sync. This reduces the chances for a sync failure and greatly reduces the time required to sync. The default sync interval is four hours.

Periodic differential sync fails if the system time on Ivanti EPMM is not in sync with the system time on the Exchange server. Ensure that the system time on Ivanti EPMM and the Exchange server are in sync. Ivanti recommends configuring an NTP server on Ivanti EPMM.

The sync interval for differential sync for Integrated Sentry can be configured in the Ivanti EPMM Admin Portal. In the Admin Portal, go to **Services > Sentry > Preferences**, and set the Sentry Sync Interval to the preferred interval.

See also, "Setting the Integrated Sentry Sync Interval" on page 146.

Manually resyncing Integrated Sentry with Exchange

You may need to perform a manual resync if you need to sync the data on Integrated Sentry immediately, before a scheduled periodic differential sync or full sync is due. If a sync is already in progress, your request for manual sync will be dropped. You will see a message saying that a sync is already running.

When you perform a manual resync, you can choose to do either a differential sync or a full sync. In most cases, you will only need to do a differential sync. Full sync is automatically triggered even when you select differential sync in the following cases:

- new access control rules were configured on the Exchange server
- changes were made to the default policy on the Exchanged server to allow or block devices
- new security policy was configured on the Exchange server

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services > Sentry**.
2. Select the **Integrated Sentry** entry.
3. Click **Resync Integrated Sentry with Exchange**.
4. In the pop-up box, select one of the following options:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Option	Description
Differential: Devices updated since last Resync (Recommended)	Integrated Sentry checks for any changes in devices or mailboxes and only updates any changes since the last successful sync. Each successful sync is timestamped. Even if there are no changes to update, the timestamp is updated to the latest successful sync.
Full: All devices	Integrated Sentry performs a batched sync for the entire list of mailboxes and devices on the Exchange server.

5. Click **Resync**.

Recalculate Integrated Sentry Office 365 mailboxes

When Integrated Sentry syncs with Office 365, Integrated Sentry now automatically requests a recalculation of the mailboxes to set the **HasActiveSyncDevicePartership** flag correctly for mailboxes that should be synced. If a mailbox has an associated mobile device, the **HasActiveSyncDevicePartership** flag is set as true. Integrated Sentry syncs only mailboxes that have the flag set as true, and ignores mailboxes that have the flag set as false.

Integrated Sentry’s request for recalculating the mailboxes ensures that the **HasActiveSyncDevicePartership** flag is set correctly for all mailboxes.

Integrated Sentry ignores mailboxes that have the **HasActiveSyncDevicePartership** flag set as false, thus increasing the efficiency of the sync.

- "Recalculate mailbox states with Office 365" below
- "Migration from Exchange to Office 365" on the next page
- "Managing the service account" on the next page
- "Troubleshooting" on the next page

Recalculate mailbox states with Office 365

To recalculate mailbox states, Integrated Sentry runs the following command from an authenticated PowerShell session connected to your Office 365 tenant:

```
"Get-CASMailbox -RecalculateHasActiveSyncDevicePartnership"
```

The recalculation should take no longer than a few seconds to run. Recalculate mailboxes with Office 365 is enabled by default. Administrative action is not required.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Migration from Exchange to Office 365

For devices migrating from Exchange to Office 365, the flag may be set incorrectly. Recalculating resets the flag to the correct value. In an environment in which mailboxes are gradually migrated to Office 365, the mailboxes will have to be regularly recalculated.

The recalculation runs in the background. Device users will not be impacted when mailboxes are recalculated. Administrative actions like adding and deleting mailboxes, and registering devices will not be impacted.

Managing the service account

The user account that you use to run the Integrated Sentry installer is also used by the Integrated Sentry service, which is a Windows service. If the user account needs a password change, make sure to update the service with the new credentials. Connectivity to Ivanti EPMM is not affected.

Procedure

1. In the Windows Control Panel, select **System And Security > Administrative Tools**.
2. Double-click **Services**.
3. Double-click the **Integrated Sentry** service.
4. Select the Log On tab and change the password.
5. Click **OK**.
6. Right-click the Integrated Sentry service and select **Restart**.

Changing the user account itself can disrupt the service. Therefore, if you want to change the service user account, uninstall and reinstall the Integrated Sentry with the new account.

Troubleshooting

Integrated Sentry creates a log file called mi-logfile.txt. The log file is located in the Integrated Sentry’s installation directory, which you selected when running the installer. By default, the log file is in the following location:

C:\Program Files (x86)\MobileIron\MobileIron Integrated Sentry\mi-logfile.txt

Integrated Sentry errors also are reported in the Admin Portal under Services > Sentry, in the Error(s) field for each Sentry.

If reporting a problem to Technical Support, include the log file and the error message along with a description of the problem.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry for ActiveSync Email

The following describe how to configure Standalone Sentry for ActiveSync email:

Overview of configuring Ivanti Standalone Sentry for email

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

You configure Ivanti Standalone Sentry for email in the Ivanti EPMM Admin Portal. Configuring Ivanti Standalone Sentry for email is a two-step process.

1. Configure an Ivanti Standalone Sentry for ActiveSync in the Ivanti EPMM Admin Portal.
2. Create an Exchange setting in the Ivanti EPMM Admin Portal, which points to the Ivanti 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.

Configuring Ivanti Standalone Sentry for ActiveSync

Before you begin

You must have installed Ivanti Standalone Sentry. For information about installing Ivanti Standalone Sentry, see the *Ivanti Standalone Sentry Installation Guide*.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services > Sentry**.
2. Select **Add New > Ivanti Standalone Sentry** or click the Edit icon for an existing Ivanti Standalone Sentry entry.
3. Complete the fields in the form for configuring ActiveSync.
4. Click **Save**.
5. Create an Exchange setting that points to the Ivanti Standalone Sentry.

Related topics

- See the following section to complete the fields in the Standalone Sentry form for configuring ActiveSync:

- "Ivanti Standalone Sentry connectivity settings" below
- "Enable ActiveSync" below
- "Configure device authentication" on the next page
- "Configure ActiveSync" on the next page
- "Configured settings for managing multiple servers" on page 44
- "Advanced settings" on page 45

- See "Configuring Exchange settings for Ivanti Standalone Sentry for ActiveSync" on page 46 to create an exchange setting.

- See "Multiple ActiveSync domains" on page 47 if Standalone Sentry will support multiple ActiveSync domains.

Ivanti Standalone Sentry connectivity settings

Enter the connectivity settings as described in the following table:

TABLE 4. IVANTI STANDALONE SENTRY CONNECTIVITY SETTINGS

Item	Description
Sentry Host / IP	Enter the host name or IP address of the server on which Ivanti Standalone Sentry is installed.
Sentry Port	Enter the port that Ivanti EPMM will use to access Ivanti Standalone Sentry. The default is 9090.

Enable ActiveSync

In the Ivanti Standalone Sentry form, select **Enable ActiveSync**. The **ActiveSync Configuration** section displays.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configure device authentication

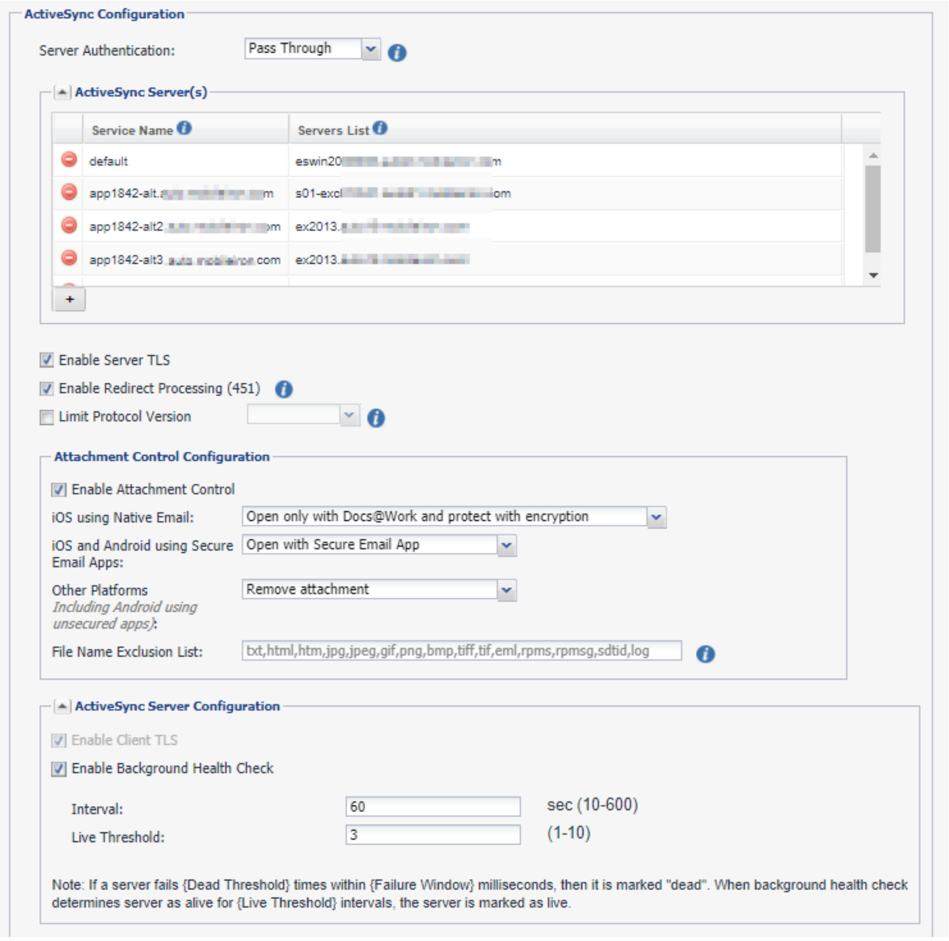
The Device Authentication setting, in the Ivanti Standalone Sentry form, determines how users attempting to connect to the ActiveSync server or backend resource authenticate with Ivanti Standalone Sentry.

See "Device and Server Authentication" on page 109 for information on selecting and configuring a method of device authentication.

See "Multiple trusted root certificates for device authentication" on page 122 for information on uploading multiple trusted root certificates for device authentication.

Configure ActiveSync

FIGURE 1. ACTIVESYC FIELDS



ActiveSync Configuration

Server Authentication: Pass Through

ActiveSync Server(s)

Service Name	Servers List
default	eswin20[redacted]m
app1842-alt.[redacted]m	s01-excl[redacted]om
app1842-alt2[redacted]om	ex2013.[redacted]
app1842-alt3[redacted].com	ex2013.[redacted]

☑ Enable Server TLS

☑ Enable Redirect Processing (451)

☐ Limit Protocol Version

Attachment Control Configuration

☑ Enable Attachment Control

iOS using Native Email: Open only with Docs@Work and protect with encryption

iOS and Android using Secure Email Apps: Open with Secure Email App

Other Platforms *Including Android using unsecured apps)*: Remove attachment

File Name Exclusion List: txt,html,htm,jpg,jpeg,gif,png,bmp,tiff,tif,eml,rpms,rpmsg,sdtid,log

ActiveSync Server Configuration

☑ Enable Client TLS

☑ Enable Background Health Check

Interval: 60 sec (10-600)

Live Threshold: 3 (1-10)

Note: If a server fails {Dead Threshold} times within {Failure Window} milliseconds, then it is marked "dead". When background health check determines server as alive for {Live Threshold} intervals, the server is marked as live.

Use the guidelines in the following table to configure ActiveSync.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Table 5. ActiveSync configuration settings

ActiveSync Configuration **This section of the form displays only if you choose Enable ActiveSync.**	
Server Authentication	Select how Sentry authenticates the user to the ActiveSync server. Select Pass Through or Kerberos. The Kerberos option is only available if you selected Identity Certificate for Device Authentication. If you select Kerberos, the Kerberos Authentication Configuration section displays. See "Configuring authentication using an identity certificate and Kerberos constrained delegation" on page 116 for information on configuring Kerberos for server authentication.
ActiveSync Server(s)	
ActiveSync Service	The first entry is always **default** and cannot be edited. You can add multiple ActiveSync services. You configure multiple ActiveSync services if your enterprise has multiple Exchange ActiveSync (EAS) domains, and you want to use the same Standalone Sentry as the gatekeeper to the ActiveSync domains. For more information on configuring multiple EAS domains on the same Standalone Sentry, see "Multiple ActiveSync domains" on page 47. If you are configuring multiple ActiveSync services, enter the hostname for the Standalone Sentry. The hostname you enter here should match the hostname in the DNS entry that resolves to the Standalone Sentry IP address. The service name cannot contain the following characters: /;?*<>|” or space. Ivanti Standalone Sentry matches the Host header value (**Server Name** in the Exchange setting) to the ActiveSync **Service Name** configured in the Ivanti Standalone Sentry settings to determine which ActiveSync server to forward the traffic. If Standalone Sentry does not find a match, ActiveSync traffic is forwarded to the ActiveSync server configured in the **default** service.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 5. ACTIVESYNC CONFIGURATION SETTINGS (CONT.)

Servers List	Enter the ActiveSync server hostnames or IP addresses with port, separated by semicolons (;). The port is optional. The ActiveSync servers in this list provide failover support for each other. Sentry does scheduling and background health check on the servers listed here. The maximum number of characters accepted is 4000 characters. For Microsoft Office 365, enter outlook.office365.com. For Gmail, enter m.google.com.
Enable Server TLS	Specify whether the ActiveSync servers require SSL (i.e., port 443). If you are using Google Apps via Standalone Sentry, you must check Enable Server TLS.
Enable Redirect Processing (451)	To disable redirect processing, clear the check box. If Enable Redirect Processing (451) is disabled, the Standalone Sentry does not handle redirection, and passes the redirect URL to the device. See also "451 redirect processing" on page 49.
Limit Protocol Version	Check this option to choose the ActiveSync protocol version that the device and Microsoft Exchange use to communicate with the Ivanti Standalone Sentry. If the device is already registered, you have to push the exchange profile to the device to force the device to use the new protocol. Alternately, device users can go to iOS device **Settings > Mail > Accounts**, select the enterprise mail account, and toggle to disable and re-enable the mail account.
Attachment Control Configuration Specify whether to enable email attachment control, and then specify the type of email attachment control. For more information, see "Email attachment control with Ivanti Standalone Sentry" on page 49.	
ActiveSync Server Configuration	
Enable Client TLS	Specify whether the client must use TLS. Though the field label reads "TLS", the intended requirement is SSL.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 5. ACTIVESYNC CONFIGURATION SETTINGS (CONT.)

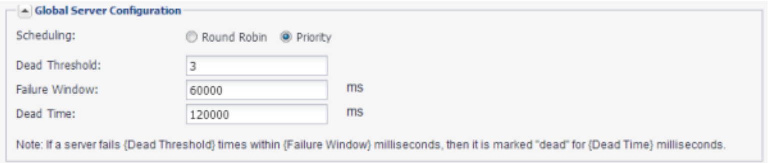
Enable Background Health Check	The default setting is enabled. Clear the check box to disable the ActiveSync server health check. If enabled, when the ActiveSync server fails for the number of times configured in the Dead Threshold setting and within the number configured in the Failure Window, then the ActiveSync server status shows Unreachable. When the background health check determines that the server is live for the number configured for Live Threshold, the ActiveSync server status shows Reachable.
Interval	Specify the time interval, in seconds, that Sentry performs a background health check. The valid range is 10 through 600. The default is 60.
Live Threshold	Specify the number of times the ActiveSync server background health check is successful before the server is marked as live. The valid range is 1 through 10. The default is 3.

Configured settings for managing multiple servers

The Global Server Configuration section in the Ivanti Standalone Sentry entry provides additional flexibility in managing multiple servers. These could be multiple ActiveSync servers or multiple enterprise resources.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 6. GLOBAL SERVER CONFIGURATION

Global Server Configuration	
 Global Server Configuration Scheduling: ○ Round Robin ● Priority Dead Threshold: 3 Failure Window: 60000 ms Dead Time: 120000 ms Note: If a server fails {Dead Threshold} times within {Failure Window} milliseconds, then it is marked "dead" for {Dead Time} milliseconds.	
Scheduling	Specify Priority or Round Robin scheduling if multiple servers are specified. Priority means that 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. Round Robin means that each server in the list will be used in turn.
Dead Threshold	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.
Failure Window	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 though 86400000 milliseconds (24 hours).
Dead Time	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).

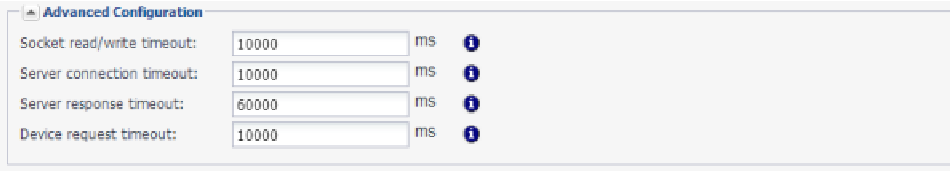
Advanced settings

The Advanced Configuration section in the Ivanti Standalone Sentry entry provides additional flexibility to configure Ivanti Standalone Sentry session timeouts. You may want to configure the session timeouts to manage server resources.

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 7. ADVANCED SETTINGS

Advanced Configuration	
 Advanced Configuration Socket read/write timeout: 10000 ms Server connection timeout: 10000 ms Server response timeout: 60000 ms Device request timeout: 10000 ms	
Socket read/write timeout	Specify the time in milliseconds, 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.
Server connection timeout	Specify the time in milliseconds after which Sentry will time out when connecting to the server. Enter a valid integer. The default setting is 10000, and the minimum is 1.
Server response timeout	Specify the time in milliseconds after which 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.
Device request timeout	Specify the time in milliseconds after which 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.

Configuring Exchange settings for Ivanti Standalone Sentry for ActiveSync

The exchange settings points to the Ivanti Standalone Sentry.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Policies & Configs > Configurations > Exchange**.
2. For Server address, enter one of the following:
   - When using Integrated Sentry, set the server address to the Microsoft Exchange Server's address.
   - When using Ivanti Standalone Sentry, set the server address to the Ivanti Standalone Sentry's address.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

If you added multiple ActiveSync services, enter the DNS hostname for the Ivanti Standalone Sentry.

- When using Ivanti 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 Ivanti 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.

3. Enter the ActiveSync User Name.
4. Enter the ActiveSync User Email.
5. Enter the ActiveSync User Password.
6. If Ivanti Standalone Sentry is using Identity or Group certificate for device authentication, select the **Certificate Enrollment** entry to generate the identity certificate for the device.
7. Click Save.
8. Apply the setting to a label that includes the devices you want to allow access to your enterprise ActiveSync server.

Related topics

- See “Exchange settings” in the Ivanti EPMM Device Management Guide to complete the fields in the form.

  - See "Re-pushing Exchange settings" on page 63 to understand the impact of re-pushing an Exchange setting.

Multiple ActiveSync domains

Ivanti Standalone Sentry supports multiple ActiveSync domains. You can configure multiple ActiveSync domains on the same Ivanti Standalone Sentry to direct email traffic. You may want to configure multiple ActiveSync domains if your enterprise has multiple Exchange ActiveSync (EAS) domains and you want to use the same Standalone Sentry as the proxy to the ActiveSync domains.

Standalone Sentry gets the ActiveSync server information from the Host header in the HTTP request. The device populates the Host header with the value of the **Server Name** configured in the Exchange setting in Ivanti EPMM. Standalone Sentry matches the Host header value (**Server Name** in the Exchange setting) to the ActiveSync **Service Name** configured in the Standalone Sentry settings to determine which ActiveSync server to forward the traffic. If Standalone Sentry does not find a match, the traffic is forwarded to the ActiveSync server configured in the **default** service.

Additional setup on your domain name server (DNS) and on Ivanti EPMM is required to support multiple ActiveSync domains on Ivanti Standalone Sentry. The additional setup is described in the following sections:

- "DNS setup" on the next page
- "Ivanti Standalone Sentry configuration" on the next page
- "Exchange setting" on the next page

- "Standalone Sentry certificate" below

DNS setup

Each EAS domain must have a separate Ivanti Standalone Sentry DNS entry that points to the IP address for the Ivanti Standalone Sentry on which you are configuring the EAS domain. For example, if you have two EAS domains, myenterprise1.com and myenterprise2.com, create two Ivanti Standalone Sentry DNS entries, standalonesentry1.com and standalonesentry2.com. Point the Ivanti Standalone Sentry DNS entries to the IP address of the Ivanti Standalone Sentry on which you are configuring the EAS domains.

Ivanti Standalone Sentry configuration

You configure multiple domains by creating separate ActiveSync services in the Standalone Sentry settings in **Services > Sentry** in the Ivanti EPMM Admin Portal. For more information, see "Configure ActiveSync" on page 41.

- Settings in the Ivanti Standalone Sentry configuration are applied to all ActiveSync services configured in the Ivanti Standalone Sentry configuration.
- For device and server authentication, Kerberos authentication to the ActiveSync server is not supported if multiple ActiveSync services are configured.

Exchange setting

For each Ivanti Standalone Sentry DNS entry, create a corresponding Exchange setting on Ivanti EPMM. For **Server Address** in the Exchange setting, enter the DNS name for Ivanti Standalone Sentry. For more information, see "Configuring Exchange settings for Ivanti Standalone Sentry for ActiveSync" on page 46.

Standalone Sentry matches the hostname in the Exchange setting to the **ActiveSync Service** name in the Standalone Sentry configuration. The ActiveSync traffic is forwarded to the ActiveSync servers configured for that service. If the hostname entered in the Exchange setting does not match any ActiveSync service name configured on Standalone Sentry, the **default** service is used, and traffic is routed to the ActiveSync server associated with the **default** service.

Standalone Sentry certificate

Upload a separate Standalone Sentry certificate for each Standalone Sentry DNS entry, so that devices can trust the Standalone Sentry. Alternately, you can also do the following:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Upload a wild card certificate that covers the domains for all ActiveSync services on Standalone Sentry.

OR

- Upload a certificate with one or more SAN names that cover the DNS Names of all ActiveSync services on Standalone Sentry.

You upload the Standalone Sentry certificate in the Ivanti EPMM Admin Portal. Go to **Services > Sentry**, and click the **Manage Certificate** link. For more information, see "Uploading Sentry certificates" on page 150.

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 Ivanti Standalone Sentry by enabling or disabling the **Enable Redirect Processing (451)** field in the **Edit Standalone Sentry** page. From the Admin Portal, go to **Services > Sentry**, and click on the edit icon for the Sentry. Redirect processing is enabled by default. To disable redirect processing clear the checkbox next to **Enable Redirect Processing (451).**

Email attachment control with Ivanti Standalone Sentry

Email attachment control determines if and how mobile devices view email attachments. The default setting for Attachment Control is disabled. If Attachment Control is set to disabled, Standalone Sentry delivers attachments as is to all devices.

Up to four emails embedded within the email are supported. All attachment control options are supported for each of the embedded emails. If an email contains five or more levels of embedded emails, Sentry encrypts/converts all attachments, including text and image files.

The following provide additional information about email attachment control with Ivanti Standalone Sentry:

- "Email attachment control support" on the next page
  - "Email attachment control options" on the next page
  - "Remove attachment" on page 51
  - "Open Only with Docs@Work and Protect with Encryption" on page 52
  - "Deliver as is" on page 53
  - "Open with Secure Email App" on page 54

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- "Forward emails with attachments" on page 54
- "Attachment control recommendation for multiple Sentrys" on page 54
- "Default file name exclusion list" on page 55
- "Standalone Sentry S/MIME handling to sign or encrypt emails" on page 56

Email attachment control support

Ivanti Standalone Sentry supports email attachment control only for the iOS native email client, and some AppConnect-enabled email apps. If you are using attachment control, and some iOS devices use other third-party iOS email clients for which attachment control is not supported, configure a separate Sentry for those devices. On that Sentry, do not enable attachment control.

Android devices using unsecured email apps have limited email attachment control support. You can configure the Ivanti Standalone Sentry to remove the attachment or to deliver the attachment as is, without added security. However, for secure, AppConnect-enabled email apps on Android devices, you can configure Ivanti Standalone Sentry to deliver the attachment for the secure app to open in the secure container.

Email apps on Windows devices have limited email attachment control support. You can configure Ivanti Standalone entry to remove the attachment or to deliver the attachment as is, without added security.

Email attachment control options

For each Ivanti Standalone Sentry, you configure email attachment control in the Admin Portal. The following table summarizes the email attachment control options that are supported on different devices:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 8. EMAIL ATTACHMENT CONTROL OPTIONS

Email attachment control option	iOS devices using the iOS native email client	iOS devices using supported AppConnect-enabled email apps	Android devices using supported AppConnect-enabled email apps	Other Platforms (Including Android using unsecured apps)
"Remove attachment" below	Supported, but typically not used	Supported, but typically not used	Supported, but typically not used	Supported
"Open Only with Docs@Work and Protect with Encryption" on the next page	Supported	Not supported	Not supported	Not supported
"Deliver as is" on page 53	Supported, but typically not used	Not supported	Not supported	Supported
"Open with Secure Email App" on page 54	Not supported	Supported	Supported	Not supported

Remove attachment

The “Remove attachment” option causes the Ivanti Standalone Sentry to remove attachments from emails, replacing each attachment with another file. The name of the replacement file is the original attachment file name appended with removed.html. For example, myDocument.pdf is replaced with myDocument.pdf.removed.html.

The replacement file contains the following text message:

“The original attachment was removed as required by the security policies of your administrator.”

On iOS devices, the message is translated according to the language setting of the device. The language defaults to United States English if the language setting is not one of the supported languages.

Typically, you won’t use this option on iOS devices with native email or supported AppConnect-enabled email apps or on Android devices that use secure apps. Other options are available on these devices that are less intrusive, but still keep the attachments secure.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Open Only with Docs@Work and Protect with Encryption

The following describe how the option works:

- "About open only with Docs@Work and protect with Encryption" below
    - "Limitations" on the next page
    - "When to use encryption" on the next page
    - "Configuration considerations" on the next page

About open only with Docs@Work and protect with Encryption

Ivanti Standalone Sentry encrypts the email attachments. Either a .secure (128-bit encryption) or a .attachctrl (256-bit encryption) extension is appended to the attachment’s file name.

The encrypted attachments open only in the Docs@Work app. The user cannot open the attachment using any other app on the device.

Docs@Work cannot display encrypted files in the following cases:

- The file type is unsupported.

  In this case, an error message is presented when the user tries to view the attachment.

- Its encryption key does not match the attachment’s encryption key.

Docs@Work app encrypts the document when the device user sends the document as an email attachment. Either a secure (128-bit encryption) or a .attachctrl (256-bit encryption) is appended to the attachment’s file name.

- If the encrypted attachment is emailed to a work account, the recipient receives an encrypted attachment. The encrypted attachment can be opened only Docs@Work.

- If the encrypted attachment is emailed to a non-work account, Ivanti Standalone Sentry decrypts the attachment and an unencrypted attachment is sent to the non-work account. However, because the email goes through Sentry, you have a record of the email and the attachment being sent.

Already encrypted attachments (.secure or .attachctrl) emailed from a non-work account to a non-work recipient are not readable by the recipient. Since emails from non-work accounts do not go through Sentry, Sentry does not decrypt the attachment.

The following table summarizes when the recipient receives an encrypted attachment and whether the attachment is readable.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 9. ENCRYPTION BEHAVIOR FOR ATTACHMENTS

	To work colleague	To non-work colleague
From work account Attachment is encrypted	• Encrypted • Readable	• Not encrypted • Readable
From non-work account An encrypted attachment is forwarded	• Encrypted • Readable	• Encrypted • Not readable

Limitations

Consider the case where you change attachment control handling on Ivanti EPMM to no longer be **Open only with Docs@Work and protect with encryption**. When Ivanti Standalone Sentry sends subsequent emails to devices, it no longer encrypts the emails. However, the devices continue to encrypt Docs@Work attachments in emails that the user sends. If the recipient is a work colleague, the recipient can still read the attachment in Mobile@Work. However, non-work recipients cannot read the attachment. The reason is that the Ivanti Standalone Sentry no longer decrypts the attachment in the sent email.

When to use encryption

The encryption protection provides additional access control for the attachment, making it prohibitively difficult for a malicious app to view the content. However, encryption protection has an impact to Ivanti Standalone Sentry performance.

Therefore, use the encryption option only if you are operating in a high security environment.

Configuration considerations

Changing to or from this option may require you to re-push the Exchange app setting to the Ivanti Standalone Sentry’s devices. For more information, see "Impact of changing the encryption option" on page 59.

This option only works with the Docs@Work app for iOS. To implement **Open Only with Docs@Work and Protect with Encryption**, you must also configure Docs@Work.

Deliver as is

The **Deliver as is** option delivers all email attachments in their original form. The device user views attachments with any available apps that work with the type of attachment.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Typically, you won’t use this option on iOS devices using the native email client because other options that keep the attachments secure are available.

Open with Secure Email App

Typically, you use this option on:

- Android devices for which you have enabled secure apps and are using a supported AppConnect-enabled secure email app. This option delivers attachments to the secure AppConnect container. Only AppConnect apps can open the attachment.
- iOS devices using a supported AppConnect-enabled email app. This option delivers attachments to the email app.

For more information about AppConnect apps, see the AppConnect and AppTunnel Guide.

Forward emails with attachments

When a device user forwards an email that has an attachment, the attachment in the forwarded email is the *original* attachment. However, if the ActiveSync server delivers the email to another device that Ivanti Standalone Sentry manages, Ivanti Standalone Sentry applies the email attachment control to the forwarded email’s attachment.

The exception to this behavior involves the behavior of the iOS native email client. If the email attachment control option is **Remove Attachment**, the iOS native email client forwards the replacement file, the file that contains the replacement text and has the **.removed.html** file extension. The original attachment is not forwarded. However, you typically do not use the **Remove Attachment** option on iOS devices.

Attachment control recommendation for multiple Sentrys

If you are using encryption with attachment control, Ivanti recommends that all Sentrys have **Open only with Docs@Work and protect with Encryption** enabled for **iOS using Native Email**.

The attachment control encryption key, once it is generated, is persistent on Ivanti EPMM. For the Docs@Work app, the key is pushed to the iOS device when the app does an AppConnect check in. Devices that have the encryption key will encrypt documents emailed from Docs@Work and is able to view encrypted documents in Docs@Work.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

If your deployment has multiple Sentrys and some have **Open only with Docs@Work and protect with Encryption** enabled and others do not, attachment control may fail. An encrypted document is forwarded as is by a Sentry not configured to protect with encryption. In this case, you will not be able to view the encrypted document on mobile devices that do not have an encryption key. Since the document remains encrypted, you will also not be able to view it on non-mobile devices or on non-iOS email clients.

Default file name exclusion list

The File Name Exclusion text box specifies the file extensions that you always want Ivanti Standalone Sentry to deliver as is, even though the attachment control option selected is “Open only with Docs@Work and protect with encryption”.

If the text box specifies no file extensions, the Ivanti Standalone Sentry uses the following file extensions by default for the exclusion list:

- txt
- html
- htm
- jpg
- jpeg
- gif
- png
- eml
- rpms
- rpmsg
- bmp
- tiff
- tif
- sdtid
- log

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- ics

When encryption is enabled for email attachments, the Docs@Work app encrypts all email attachments, including files in the exclusion list. However, Ivanti Standalone Sentry decrypts the attachment and forwards it as an unencrypted file.

The following table summarizes how the exclusion list impacts whether the Ivanti Standalone Sentry applies each attachment control option:

TABLE 10. EXCLUSION LIST IMPACT ON ATTACHMENT CONTROL

	File extensions in exclusion list	File extensions not in exclusion list
Open only with Docs@Work and protect with encryption	Option not applied. Any appropriate app can open the file, which Sentry delivers as is.	Applied. Files open only with Docs@Work and are protected with encryption.
Remove Attachment	Applied. Sentry removes the attachment.	Applied. Sentry removes the attachment.
Deliver as is	Applied. Sentry delivers the attachment as is.	Applied. Sentry delivers the attachment as is.
Open with Secure Email App	Applied. Only secure email apps can open the attachment.	Applied. Only secure email apps can open the attachment.

Standalone Sentry S/MIME handling to sign or encrypt emails

- "Digitally signed emails" below
- "Encrypted emails" on the next page

Digitally signed emails

Most email apps can use S/MIME (Secure/Multipurpose Internet Mail Extensions) to digitally sign an email, if the email user requests it. The receiving email app processes this email signature to validate the following:

- The sender’s identity

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Whether the email has been tampered with

The Ivanti Standalone Sentry does some processing on each email that is directed to an ActiveSync device when the email attachment control option is one of the following:

- Open only with Docs@Work and protect with encryption
- Remove attachment

This processing breaks the security of the email signature. Therefore, when an email app receives a signed email in these cases, the app always indicates to the user that it cannot validate the sender’s identity and that the email has been tampered with.

For example, the iOS native email client displays the email’s From field in red if:

- an iOS device user has enabled S/MIME in the iOS Mail app
- the iOS native email client receives an S/MIME email through Standalone Sentry
- the email attachment control option is one of the options mentioned above

Encrypted emails

S/MIME can also be used to encrypt emails, although this use of S/MIME is not common. Ivanti Standalone Sentry passes along an S/MIME encrypted email with no impact to the email.

Configuring email attachment control

Use the Admin Portal to configure email attachment control.

Before you begin

- If you require different options for different users, use a different Ivanti Standalone Sentry for each set of users.
- If you plan to encrypt email attachments, **Open only with Docs@Work and protect with encryption** option for iOS devices, you must also configure the Docs@Work app.

  Make sure you have checked Enable Docs@Work in the Admin Portal, **Settings > Preferences**. For a description of email attachment control options, see "Email attachment control options" on page 50.

- For a list of supported secure email apps, see the *Standalone Sentry Release Notes*.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. Go to **Services > Sentry** in the Admin Portal.
2. Click the **Edit** icon for the Ivanti Standalone Sentry entry configured for ActiveSync.
3. Select **Enable Attachment Control**.

This option is available only if you selected **Enable ActiveSync**.

Not selecting this option means the Ivanti Standalone Sentry delivers attachments as is to all devices.

4. For **iOS Using Native Email,** select the type of attachment control that you want to use.
5. For **iOS And Android Using Secure Apps**, select the type of attachment control that you want to use.
6. For **Other Platforms (Including Android Using Unsecured Apps)**, select the type of attachment control that you want to use.

This option does not impact iOS devices at all.

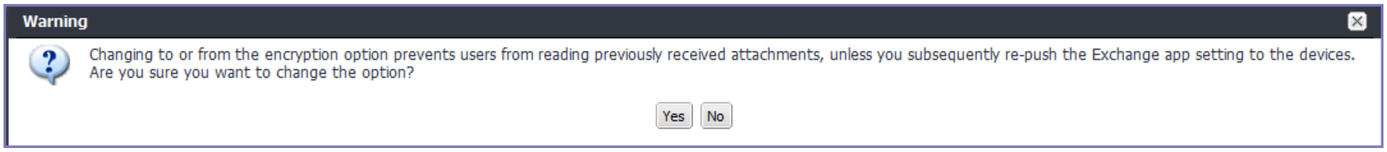
7. For **File Name Exclusion List**, enter any file extensions that you always want Ivanti Standalone Sentry to deliver as is, regardless of the attachment control option selected. Specify a comma-separated list.

If you make no entry into the text box, the default file name extension list is applied.

8. Click **Save**.
   The Standalone Sentry restarts when you click **Save.** A restart can cause a brief interruption in email service to device users.

If you changed to or from the option **Open only with Docs@Work and protect with encryption**, you will see the following warning:

FIGURE 1. WARNING MESSAGE DUE TO ENCRYPTION OPTION CHANGES



Warning

Changing to or from the encryption option prevents users from reading previously received attachments, unless you subsequently re-push the Exchange app setting to the devices.
Are you sure you want to change the option?

9. Click **Yes** if you understand and agree to the impact.

Next steps

Go to "Checking for configuration errors" on the next page.

Related topics

- "Impact of changing the encryption option" on the next page.
  - "Regenerating the encryption key" on the next page.
  - "AES-256-GCM encryption for email attachments " on page 60.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Checking for configuration errors

If the Ivanti Standalone Sentry is not available when you click **Save**, it does not receive the new settings. You can check if the changes were applied to Standalone Sentry.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services > Sentry**.
2. If there are errors, click **View Errors** on Ivanti Standalone Sentry's setting for the detailed error message.

When the Ivanti Standalone Sentry is available again, open the **Edit Standalone Sentry** view and click **Save** to send the new settings.

Impact of changing the encryption option

Changing the option from **Open only with Docs@Work, and protect with encryption** to a different option prevents iOS device users who use the iOS native email client from reading previously received attachments. If device users need to read previously received attachments, re-push the Exchange setting to the devices. Ivanti advises caution when re-pushing the Exchange setting. Re-pushing the Exchange setting increases the load on the Exchange server.

Change to or from the encryption option only if:

- you can make the change during a planned maintenance period or non-peak operating hours.
- you have notified users about what to expect.

Regenerating the encryption key

Standalone Sentry uses an encryption key to encrypt email attachments when the attachment control option is **Open only with Docs@Work, and protect with encryption.** Ivanti EPMM generates the encryption key the first time you select the encryption option. Ivanti EPMM provides one encryption key to all Standalone Sentrys using the encryption option.

Regenerate the encryption key only if:

- the key has been compromised.

  The encryption key is compromised if malicious third-party apps are using it to view email attachments.

- you are switching from AES-128-bit encryption to AES-256-bit encryption.

  "AES-256-GCM encryption for email attachments " on the next page

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- you can regenerate the key during a planned maintenance period or non-peak operating hours.
- you have notified users about what to expect.
- Key regeneration causes a restart for all Standalone Sentrys that are using encryption for attachment control.

A restart can cause a brief interruption in email service to device users.

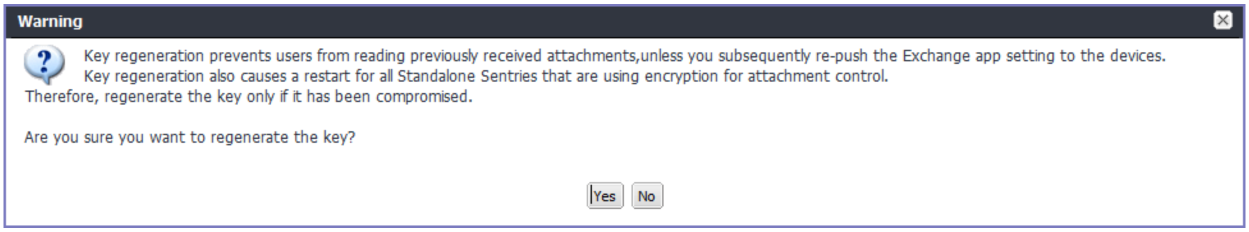
- Key regeneration prevents iOS device users who use the iOS native email client from reading previously received attachments.

Previously received attachments are encrypted with the old key, but Mobile@Work and the Docs@Work app use the new key after key regeneration. Therefore, they cannot display the old attachment. Furthermore, consider the scenario when a device user forwards an email with an attachment encrypted with the old key.The Standalone Sentry is unable to decrypt the attachment because it is using the new key. In this case, the Ivanti Standalone Sentry replaces the attachment with a text file with an explanatory message.

Procedure

1. In the Admin Portal, go to **Services > Sentry > Preferences**.
2. In the **Standalone Sentry** section, click **Regenerate Key**.

FIGURE 2. KEY REGENERATE WARNING



Key regeneration prevents users from reading previously received attachments,unless you subsequently re-push the Exchange app setting to the devices.
Key regeneration also causes a restart for all Standalone Sentries that are using encryption for attachment control.
Therefore, regenerate the key only if it has been compromised.

Are you sure you want to regenerate the key?

3. Click **Yes** if you are sure you want to regenerate the key.

If an Ivanti Standalone Sentry is not available when you regenerate the key, its entry in **Sentry > Settings** displays an error.

AES-256-GCM encryption for email attachments

Ivanti Standalone Sentry 6.1 adds support for AES-256-GCM for encrypting email attachments. If you already have Docs@Work (original) enabled and are now enabling Docs@Work, the system continues to use 128-bit encryption for email attachments.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

To use 256-bit encryption with the Docs@Work app, you must first disable Docs@Work (Original) and then regenerate the attachment encryption key. A 256-bit key is only generated if Docs@Work (Original) is disabled and all Standalone Sentry servers that are configured on Ivanti EPMM are at least Version 6.1.

TABLE 11. 256-BIT ENCRYPTION BEHAVIOR

Docs@Work (Original)	Docs@Work	Sentry Version	Encryption key generated
Enabled	Enabled	-	AES-128-ECB
Disabled	Enabled	Some Standalone Sentrys are less than Version 6.1	AES-128-ECB
Disabled	Enabled	All Sentrys are at least Version 6.1	AES-256-GCM

- Key regeneration causes a restart for all Ivanti Standalone Sentrys that use encryption for attachment control. A restart can cause a brief interruption in email service to device users.
- After regenerating the encryption key, iOS device users who use the iOS native email client cannot read previously received attachments. If device users need to read previously received attachments, re-push the Exchange setting to the devices. Ivanti advises caution when re-pushing the Exchange setting. Re-pushing the Exchange setting increases the load on the Exchange server. See "Re-pushing Exchange settings" on page 63.

Configuring AES-256-GCM encryption for email attachments

If you previously had Docs@Work (Original) enabled, attachments are encrypted with AES-128. To use 256-bit encryption, you must disable Docs@Work (Original) and enable Docs@Work.

Procedure

1. Ensure that all Sentrys configured on Ivanti EPMM are at least Version 6.1.
2. In the Admin Portal, go to **Settings** > **Preferences**.
3. Scroll down to the **Additional Products** section.
4. De-select **Enable Docs@Work (Original)**.
5. Ensure that **Enable Docs@Work** is enabled.
6. Click **Save**.
7. Go to **Services** > **Sentry**, and click **Preferences**.
8. In the **Standalone Sentry** section, click **Regenerate Key**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configuring certificate-based tunneling for IBM Verse clients on Android enterprise

You can set up certificate-based tunneling for IBM Verse clients using Standalone Sentry on Android enterprise devices. Certificate -based tunneling only supports SyncML traffic. Certificate-based tunneling does not require Ivanti Tunnel or AppConnect.

Before you begin

- Ivanti EPMM must be set up for Android enterprise. For more information, see *Ivanti EPMM Device Management Guide for Android and Android Enterprise devices*.
- Ivanti EPMM must be set up as an independent root CA. See the “Configuring Ivanti EPMM as an independent root CA (Self-Signed)” section in the *Ivanti EPMM Device Management Guide for Android and Android Enterprise devices* for information on how to create a local CA and the corresponding Local certificate enrollment setting.
- Add the following for **Subject Alternative Names** in the **Local** certificate enrollment setting:

  Type: **Uniform Resource Identifier**
  Value: cbt://*mycomp.com*?EmmUsrId=$USERID$&EmmDevId=$DEVICE_UUID&EmmCfgId=CONFIG_UUID_ANDROID_RESTRICTIONS&AppBundleId=com.ibm.lotus.traveler
  The URI scheme, cbt,, is case insensitive. *mycom.com* is the hostname and can be anything.

Ensure that the **Local** certificate enrollment setting is applied to a label containing the Android enterprise devices which will use certificate-based tunneling.

- Standalone Sentry must be enabled for AppTunnel and set up to do device authentication using Identity certificates. Upload the Ivanti EPMM local self-signed CA in Standalone Sentry settings in the Ivanti EPMM Admin Portal.
- Both Pass Through and Kerberos are supported for server authentication.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services** > **Sentry**.
2. Click the edit icon for a Standalone Sentry that is enabled for AppTunnel and configured to use Identity certificates for device authentication.
3. In the **AppTunnel Configuration** section, add an AppTunnel service in **Services**.

Item	Description
Service Name	Enter a name for the service in the following format: CBT_HTTP_*FQDNofTheSentry*.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Item	Description
	The FQDN is for the external hostname assigned to Ivanti Standalone Sentry. Example: CBT_HTTP_sentry1.mycompany.com
Server Auth	Select **Pass Through**.
Server List	Enter the backend resource’s host name or IP address (usually an internal host name or IP address). Include the port number on the backend resource that Ivanti Standalone Sentry can access. You can enter multiple servers. Standalone 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. Separate each resource name with a semicolon. Example:email1.companyname.com:443;email2.companyname.com:443
TLS Enabled	Select if the servers listed in the **Server List** field require SSL.
Proxy/ATC	Select if you want to direct the AppTunnel service traffic through the proxy server. You must also have configured **Server-side Proxy** or **Advanced Traffic Control (ATC)**.
Server SPN List	Enter the Service Principal Name (SPN) for each server, separated by semicolons.

4. Click **Save**.

Re-pushing Exchange settings

You may need to re-push the Exchange setting in some cases, such as, after you have regenerated the encryption key for attachment control.

The re-push sends the Exchange setting to *all* devices with the appropriate label, not just the iOS devices.

Ivanti advises caution when re-pushing the Exchange setting. On each affected device, the re-push causes the email app that uses the Exchange setting to:

- re-sync its emails, calendar items, tasks, and contacts. For example, the email app removes all emails from its email folders and then re-fetches the emails from the ActiveSync server.
- in some cases, prompt the device user to reenter his password for accessing email.

The easiest way to re-push an Exchange setting to a device is to make a simple change, such as adding a space at the end of the Description field. The next time each device checks in, Ivanti EPMM sends the Exchange setting to the device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Select an Exchange setting that uses the Ivanti Standalone Sentry with the changed attachment control option.
3. Click **Edit** to open the **Modify Exchange Setting** screen displays.
4. Add a space to the end of the **Description** field.
5. Click **Save**.
6. Repeat steps 2 through 5 for each Exchange setting that uses the Ivanti Standalone Sentry with the changed attachment control option.

Changing the background health check for ActiveSync servers

Ivanti Standalone Sentry performs periodic background health checks to determine if the ActiveSync server is up. Background health check is enabled by default.

Ivanti recommends disabling Background health check if you are using only one ActiveSync server or a cloud-based email service.

Procedure

1. In the Admin Portal, go to **Services > Sentry**.
2. Click on the edit icon for Sentry.
3. In the **Edit Standalone Sentry** page, under **ActiveSync Configuration**, expand **ActiveSync Server Configuration**.
4. Select the check box for **Enable Background Health Check** to enable background health check or uncheck the check box to disable background health check.
5. Click **Save**.

Related topics

- See "ActiveSync configuration settings" for a description of the setting.
  - See "ActiveSync server status" on page 260 for how to check the ActiveSync server status.

Standalone Sentry Email+ Notification Service for Ivanti EPMM

You can set up Ivanti Standalone Sentry as an Email+ Notification Service. This feature is available only when it is used with Email+ 3.13.0. This capability allows you to configure multiple Exchange servers to provide notifications for VIP accounts in Email+. This feature requires Ivanti EPMM, cloud notification service (CNS), Ivanti Standalone Sentry, and Email+.

To enable Email+ notifications, you must configure Ivanti Standalone Sentry configuration on Ivanti EPMM. You must also configure the key-value pairs in the AppConnect App configuration.

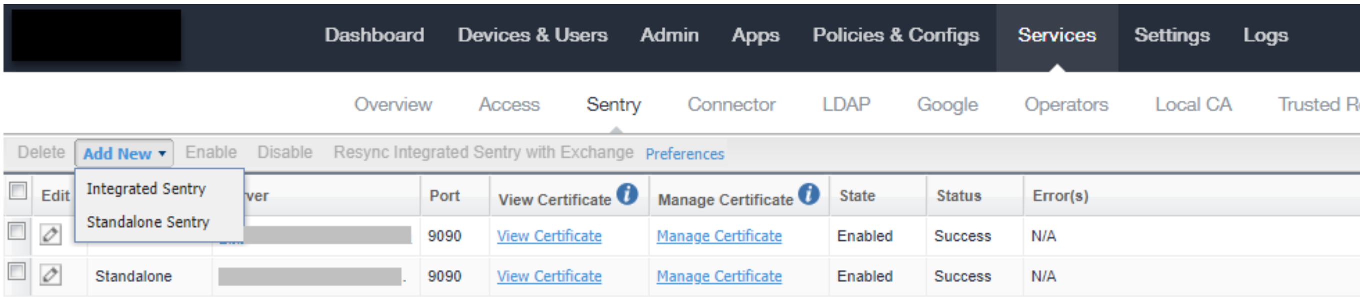
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Before you begin

- Ensure that you have Ivanti EPMM 10.5.0.2 or later and Sentry 9.8.5 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.
- Ivanti 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 68.
  Also, see Microsoft documentation.
- If Exchange server version support is earlier than TLS v1.2, then the supported protocols should be configured in Incoming protocols on MICS.
- Supported protocols are configured under Incoming SSL configuration under custom configuration on Sentry MICS UI.
- Ensure that the Ivanti Standalone Sentry port is configured at 9090 as default.

Procedure

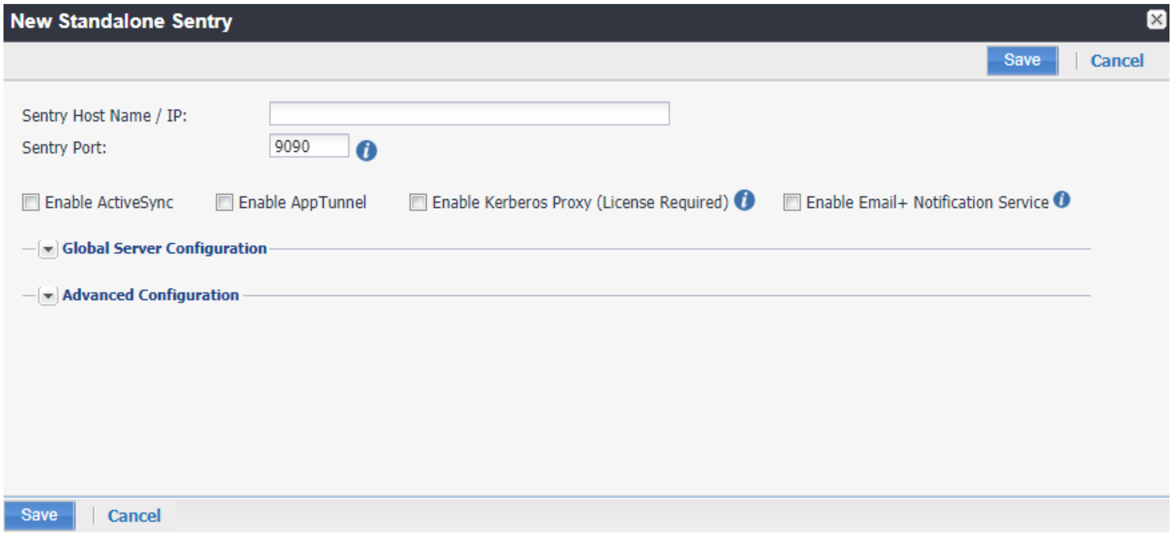
1. In Ivanti EPMM, click **Services** > **Sentry** > **Add New** > **Standalone Sentry**.



□	Edit		ver	Port	View Certificate	Manage Certificate	State	Status	Error(s)
□	✎		[redacted]	9090	View Certificate	Manage Certificate	Enabled	Success	N/A
□	✎	Standalone	[redacted]	9090	View Certificate	Manage Certificate	Enabled	Success	N/A

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

2. On the **New Standalone Sentry** window, enter the **Sentry Hostname / IP**.



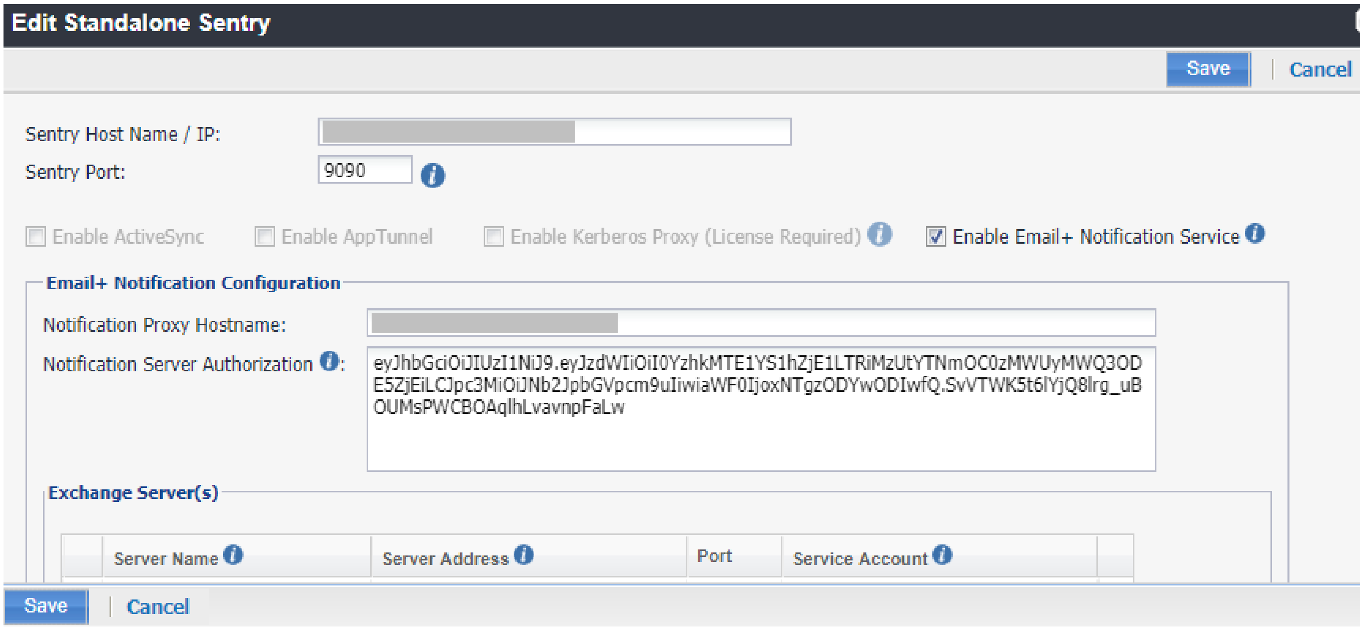
New Standalone Sentry

Sentry Host Name / IP:

Sentry Port: 9090

□ Enable ActiveSync □ Enable AppTunnel □ Enable Kerberos Proxy (License Required) □ Enable Email+ Notification Service

3. Select the **Enable Email+ Notification Service** checkbox.
 If Email+ notification is enabled, other Sentry services such as ActiveSync, App Tunnel, and Kerberos Proxy are disabled.
4. For **Notification Proxy Hostname**, enter the Sentry Hostname.
This is the same hostname you entered for Sentry Host Name.
5. For **Notification Server Authorization**, enter the CNS JWT token.
The CNS JWT token is per tenant and is different for every tenant.



Edit Standalone Sentry

Sentry Host Name / IP: [redacted]

Sentry Port: 9090

□ Enable ActiveSync □ Enable AppTunnel □ Enable Kerberos Proxy (License Required) ☑ Enable Email+ Notification Service

Email+ Notification Configuration

Notification Proxy Hostname: [redacted]

Notification Server Authorization:

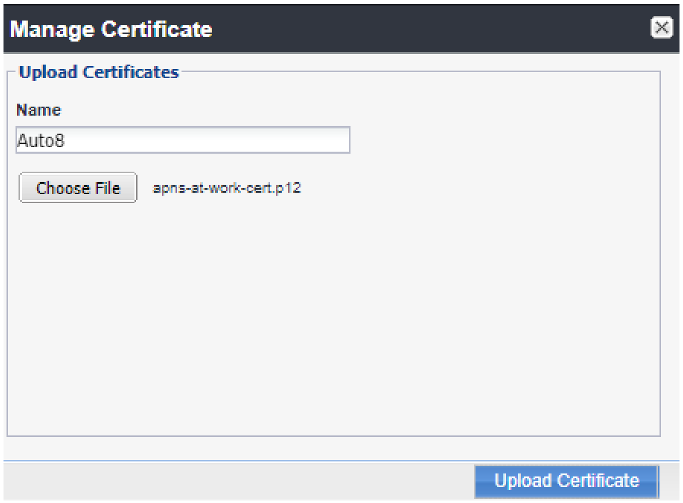
eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiI0YzhkMTE1YS1hZjE1LTRiMzUtYTNmOC0zMWUyMWQ3OD
E5ZjEiLCJpc3MiOiJNb2JpbGVpcm9uIiwiaWF0IjoxNTgzODYwODIwfQ.SvVTWK5t6lYjQ8lrg_uB
OUMsPWCBOAqlhLvavnpFaLw

Exchange Server(s)

	Server Name	Server Address	Port	Service Account	

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

6. Under **Service Account(s)**, click + . The **Manage Certificate** window appears.



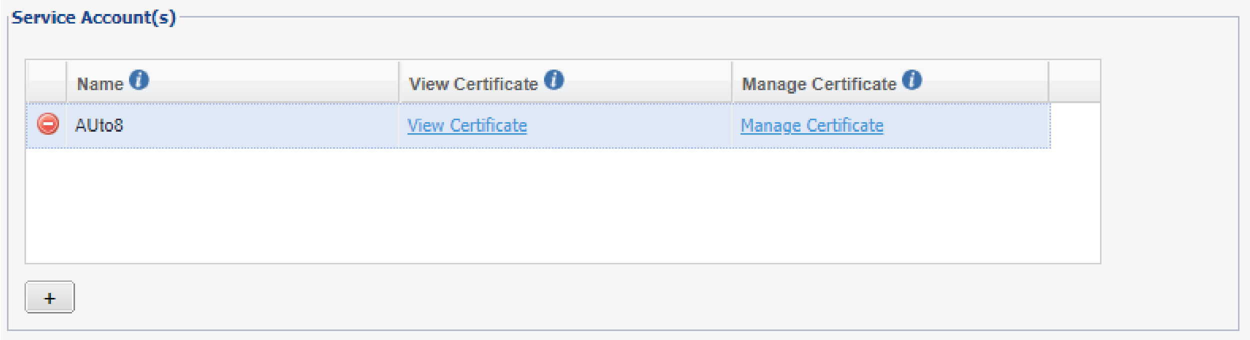
Manage Certificate

Upload Certificates

Name: Auto8

Choose File apns-at-work-cert.p12

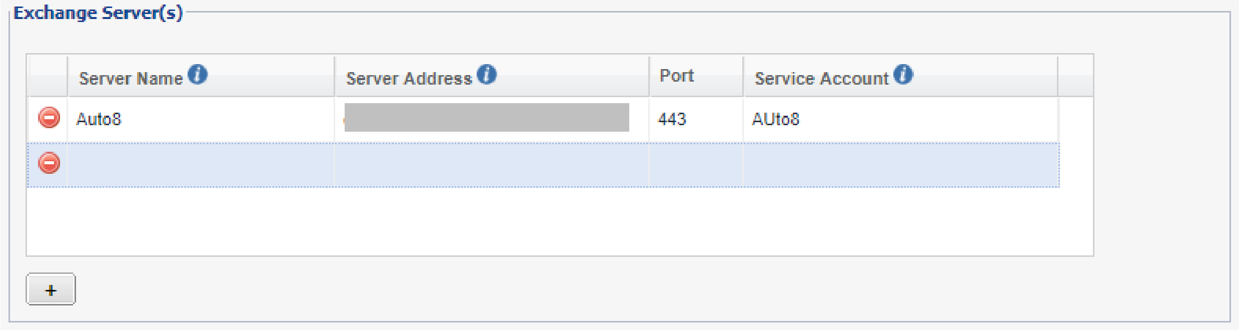
7. Enter the **Name** and click **Choose File** to upload the PKCS12 certificate to authenticate service account on Exchange server.
   Ensure that the certificate is uploaded successfully.



Service Account(s)

	Name	View Certificate	Manage Certificate
⊖	AUto8	View Certificate	Manage Certificate

8. Under **Exchange Server(s)**, click + to add the Exchange Servers.



Exchange Server(s)

	Server Name	Server Address	Port	Service Account
⊖	Auto8	[redacted]	443	AUto8
⊖				

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

9. Enter a display name for the exchange server in the **Server Name** field and in the **Server Address** field enter the server address which is the Host Name / IP Address of the Exchange server.
   The port is configured at 443.
10. Select the configured **Service Account** from the drop-down.
11. Click **Save** on the **New Standalone Sentry** screen after configuration is complete.

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.

```
<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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti EPMM with a certificate is also known as certificate-based authentication (CBA) to Ivanti EPMM.

OAuth for Sentry on Ivanti EPMM

OAuth is supported with Ivanti 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

Sentry 9.14.0 and 9.15.0 supports Azure AD Conditional Access Policy.
For more information, see "Configuring conditional access policy in Azure AD" on page 75.

Configuring Sentry on Ivanti EPMM for OAuth

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Before you begin

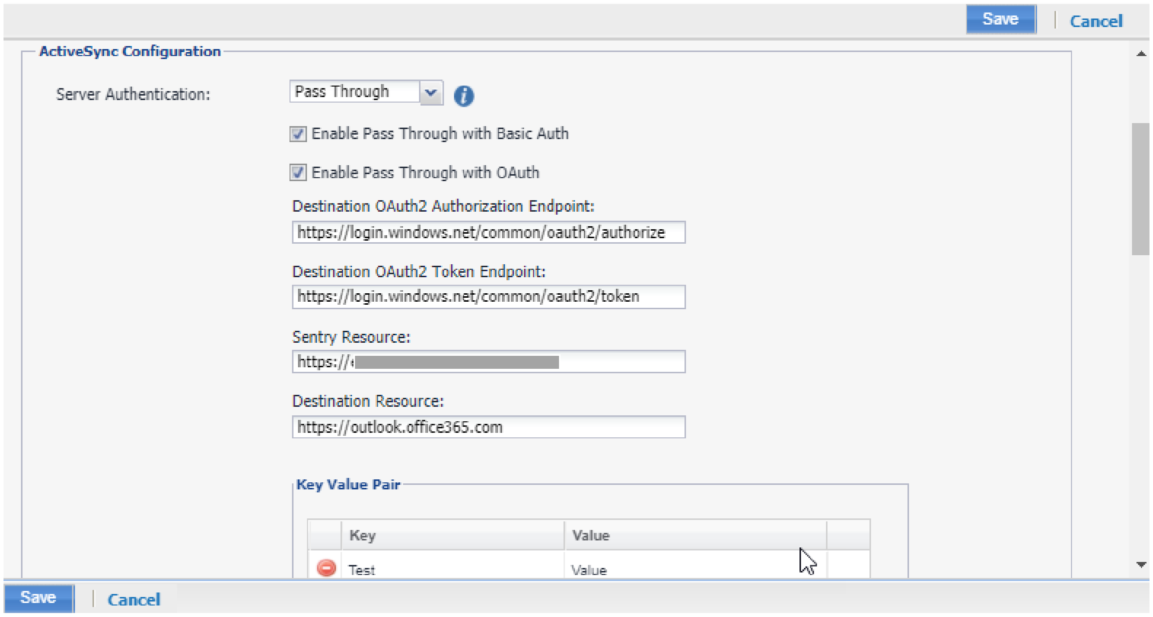
- Verify that you have Sentry 9.14.0 or later and Ivanti EPMM 11.0.0.0 or later.

Procedure

1. Login to Ivanti EPMM with admin credentials.
2. Click **Services** > **Sentry**.
3. Click **Add New** > **Standalone Sentry**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. Select **Enable ActiveSync** and enter the following details for OAuth.



ActiveSync Configuration

Server Authentication: Pass Through

☑ Enable Pass Through with Basic Auth

☑ Enable Pass Through with OAuth

Destination OAuth2 Authorization Endpoint: https://login.windows.net/common/oauth2/authorize

Destination OAuth2 Token Endpoint: https://login.windows.net/common/oauth2/token

Sentry Resource: https://[redacted]

Destination Resource: https://outlook.office365.com

Key Value Pair

Key	Value
Test	Value

   a. Select **Pass Through** for **Server Authentication**.

   b. Select **Enable Pass Through with OAuth**.

   c. **Destination OAuth2 Authorization Endpoint**: "https://login.windows.net/common/oauth2/authorize"

   d. **Destination OAuth2 Token Endpoint**: "https://login.windows.net/common/oauth2/token"

   e. **Sentry Resource**: https://<SentryHostName>

   f. **Destination Resource**: https://outlook.office365.com/
   If Active Sync servers are not added by default, then configure Active sync server as outlook.office365.com.

5. Click **Save**.

Configuring OAuth for Email+ through Sentry on Ivanti EPMM

After the iOS Email+ application is installed the configuration must be pushed to the device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Before you begin

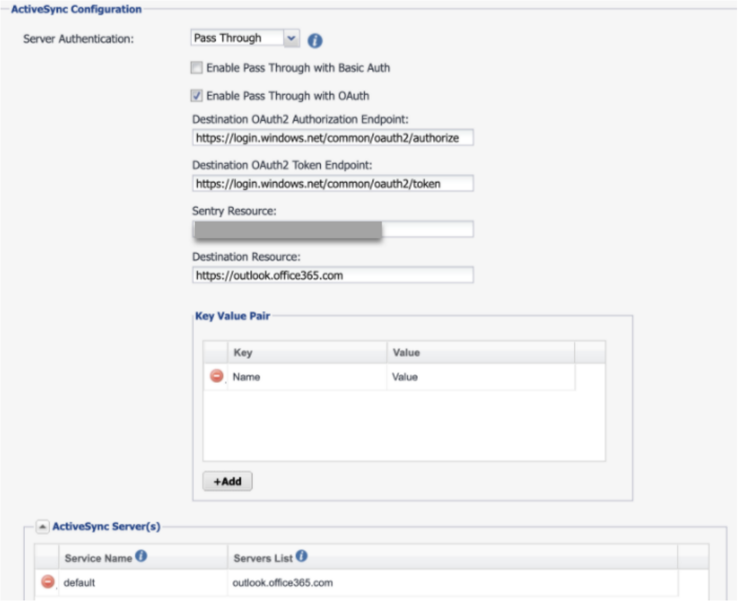
- Verify that you have installed iOS Email+ application.

Procedure

1. Login to Ivanti EPMM with admin credentials.
2. Click **Services** > **Sentry**.
3. Click **Add New** > **Standalone Sentry**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. Select **Enable ActiveSync** and enter the following details for OAuth.



ActiveSync Configuration

Server Authentication: Pass Through

☐ Enable Pass Through with Basic Auth

☑ Enable Pass Through with OAuth

Destination OAuth2 Authorization Endpoint:
https://login.windows.net/common/oauth2/authorize

Destination OAuth2 Token Endpoint:
https://login.windows.net/common/oauth2/token

Sentry Resource:
[redacted]

Destination Resource:
https://outlook.office365.com

Key Value Pair

Key	Value
Name	Value

ActiveSync Server(s)

Service Name	Servers List
default	outlook.office365.com

a. Select **Pass Through** for **Server Authentication**.

b. Select **Enable Pass Through with OAuth**.

c. **Destination OAuth2 Authorization Endpoint**: "https://login.windows.net/common/oauth2/authorize"

d. **Destination OAuth2 Token Endpoint**: "https://login.windows.net/common/oauth2/token"

e. **Sentry Resource**: https://<SentryHostName>

f. **Destination Resource**: https://outlook.office365.com/
If Active Sync servers are not added by default, then configure Active sync server as outlook.office365.com.

5. Click **Save**.

Configuring iOS native email configuration with OAuth

Before you begin

- Verify that you have enabled "**Use OAuth for Authentication**" for iOS 5 and later versions.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

With iOS 14 and newer versions, password prompts appear on the devices for iOS Native email client when the exchange profile with OAuth configuration is pushed to the devices.

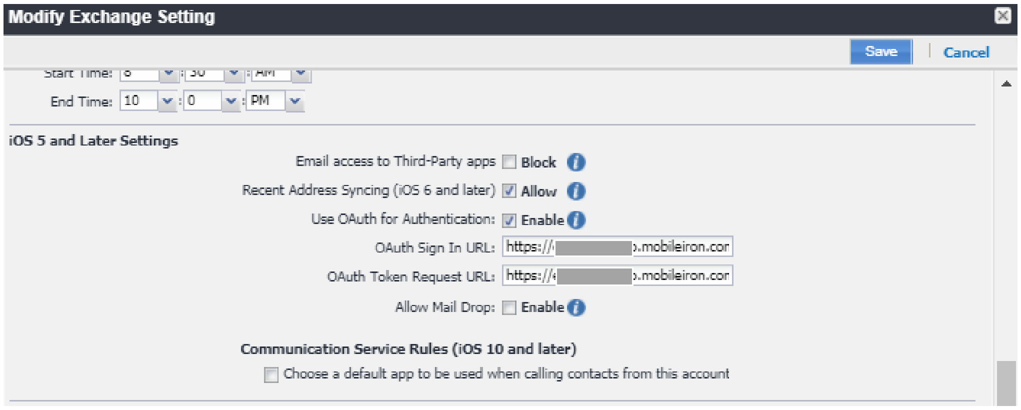
When you configure an OAuth feature, Sentry must be configured with Active Sync only and do not select AppTunnel. For AppTunnel use a different Sentry.

Procedure

1. Login to Ivanti EPMM with admin credentials.
2. Click **Policies and Configs**.
3. Click **Edit** on the exchange configuration.
4. Enable **Use OAuth for Authentication**.
5. Under **iOS 5 and Later Settings**, enter the following details:

   OAuth Sign In URL: https://<SentryHostName>/proxyservice/oauth2/authorize

   OAuth Token Request URL: https://<SentryHostname>/proxyservice/oauth2/token

   Start Time: 8 : 30 : AM

   End Time: 10 : 0 : PM

   iOS 5 and Later Settings

   Email access to Third-Party apps □ Block

   Recent Address Syncing (iOS 6 and later) ☑ Allow

   Use OAuth for Authentication: ☑ Enable

   OAuth Sign In URL: https://[redacted].mobileiron.cor

   OAuth Token Request URL: https://[redacted].mobileiron.cor

   Allow Mail Drop: □ Enable

   Communication Service Rules (iOS 10 and later)

   □ Choose a default app to be used when calling contacts from this account

6. Click **Save**.

Configuring Android and iOS Email+ with OAuth

For more information on configuring Android or iOS Email+ for OAuth, see Email+ Product Documentation.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

When you configure an OAuth feature, Sentry must be configured with Active Sync only and do not select App Tunnel. For App Tunnel use a different Sentry.

KVPs for Email+ Configuration

For OAuth, ensure to set "eas_min_allowed_auth_mode" to "modern_auth" and provide the modern_auth_authority_url and modern_auth_resource_url for appropriate OAuth configuration:

- eas_min_allowed_auth_mode: modern_auth
- modern_auth_authority_url: https://<SentryHostname>/proxyservice
- modern_auth_resource_url: https://<SentryHostname>

For OAuth Email+ CBA user, the following KVP must be provided:

- email_login_certificate = <CBACertificateName>.pfx

Configuring conditional access policy in Azure AD

You can configure the conditional access rules in Azure for OAuth to function correctly.

1. Login to Azure portal with admin credentials.
   The admin has to be super admin who has premium features to configure Conditional Access rules.
2. Click **Azure AD Conditional Access** > **Named Locations** > **IP Range Locations** > **New IP Range Location**.
3. Click **Add** and enter the IPv4 or IPv6 address range.
4. Configure a name and Sentry IP address with **Subnet** > **Add** > and enable **Mark as Trusted location** > **Create**.
5. On the **Home** tab, click **Conditional Access Policies** > **Create New Policy**.
6. Under **Users and Groups**, select Users and Groups.
7. Search for the appropriate Users or Groups and click **Select**.
8. Under **Cloud apps or actions**, select **apps** > **Office 365**.
9. Under **Conditions** > **Locations** > **Any Location** > Configure "**Yes**" under Include to "**Any Location**".

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

10. Under list of locations, select **Selected locations** under **Exclude**.

11. Select **Grant access as block access** > **require one of the selected controls**.

12. Select **Enable Policy** > **On**> **Create**.

Multi-factor authentication configuration for Ivanti EPMM

The user should be capable of using multi-factor authentication by enabling multi-factor authentication setting on Azure.

To support multi-factor authentication in Sentry OAuth, you must configure one Sentry for OAuth and another Sentry for multi-factor authentication using Tunnel.

Sentry 9.14 and 9.15 supports Azure AD Conditional Access Policy.
For more information, see Configuring conditional access rules in Azure.

Configuring multi-factor authentication on Azure

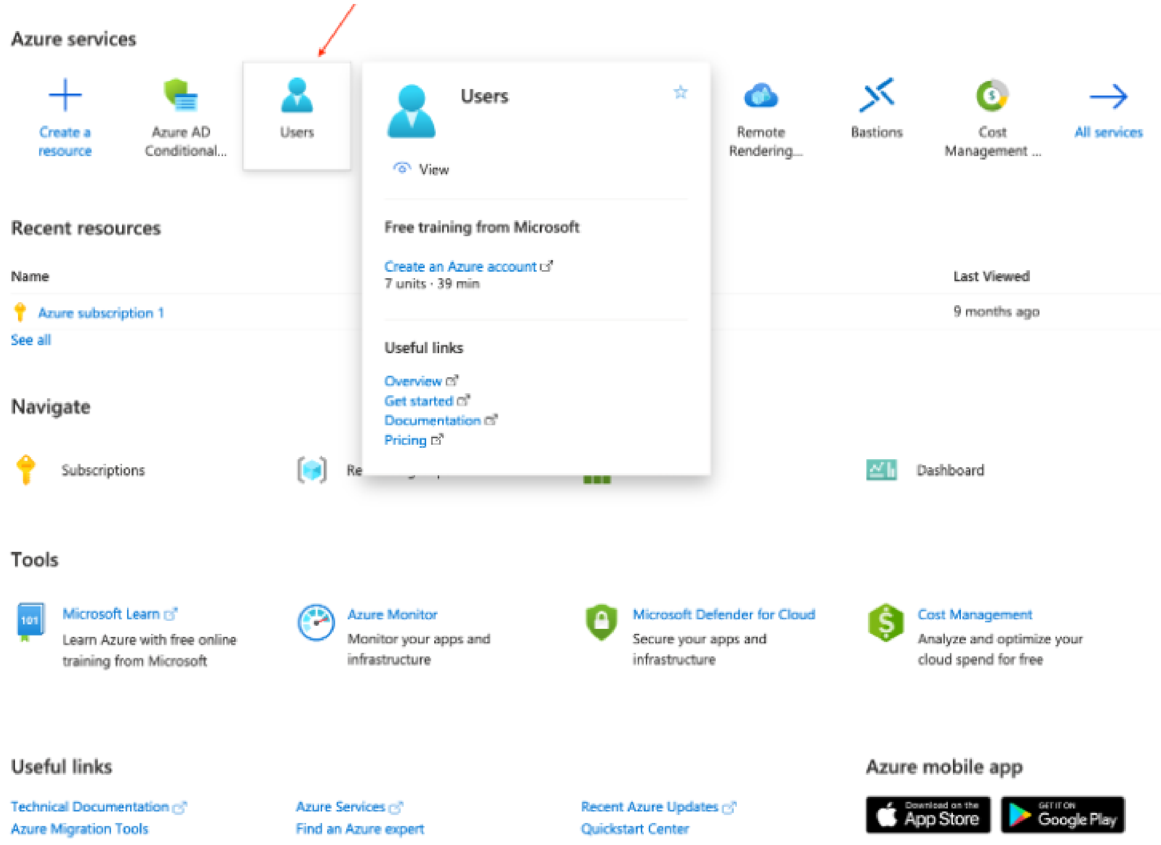
Before you begin

- Verify that you have Sentry 9.15.0 and newer versions.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

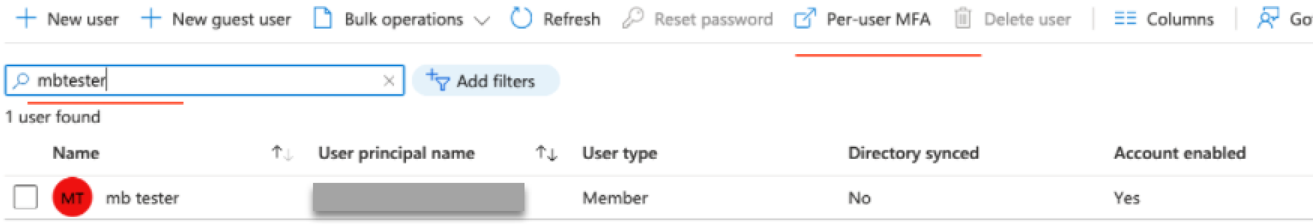
1. Login to [Azure portal]() with admin credentials.
   The admin must be a super admin with premium features to configure multi-factor authentication for other users.



2. Click **Users** and search for the user to enable multi-factor authentication.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. [Privacy and Legal]().

3. Select **Per-user MFA**.
   The multi-factor authentication page opens to configure the user.



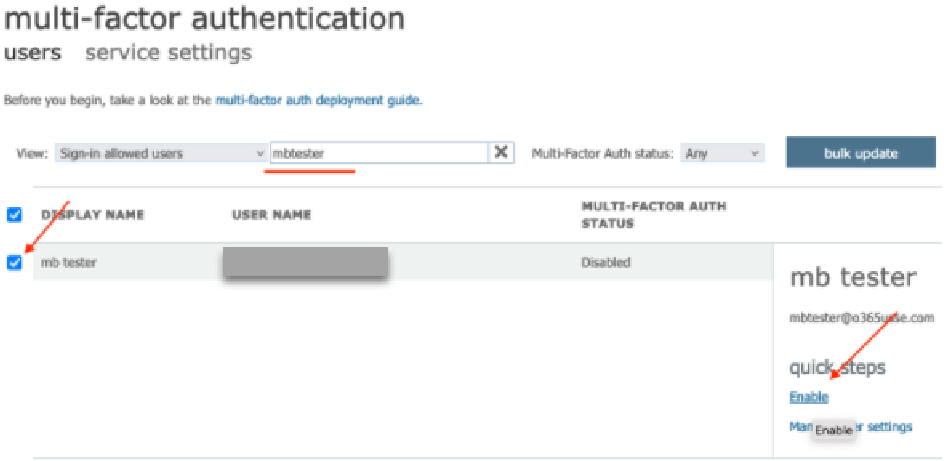
mbtester

1 user found

	Name	User principal name	User type	Directory synced	Account enabled
□	mb tester	[redacted]	Member	No	Yes

4. Select the checkbox to enable the user.
   If multi-factor authentication is not enabled, the status of multi-factor authentication shows disabled.

5. Select **Enable** in the menu on the right.



Before you begin, take a look at the multi-factor auth deployment guide.

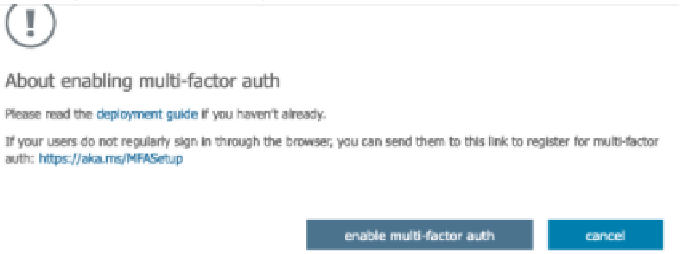
View: Sign-in allowed users mbtester Multi-Factor Auth status: Any

☑	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
☑	mb tester	[redacted]	Disabled

mb tester

mbtester@o365u[illegible]e.com

6. Enabling the user displays a prompt to enable multi-factor authentication for the specific user.



About enabling multi-factor auth

Please read the deployment guide if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

7. Click **enable multi-factor auth**.

   A confirmation message displays after enabling multi-factor authentication.

8. The user OAuth status is now changed to **Enabled**.

Configuring native email on Ivanti EPMM for multi-factor authentication

Procedure

1. On one Sentry, configure OAuth. See "OAuth for Sentry on Ivanti EPMM" on page 69.

2. On a different Sentry, configure VPN on **Ivanti EPMM** UEM.

   a. On **Ivanti EPMM**, click **Policies and Config**.

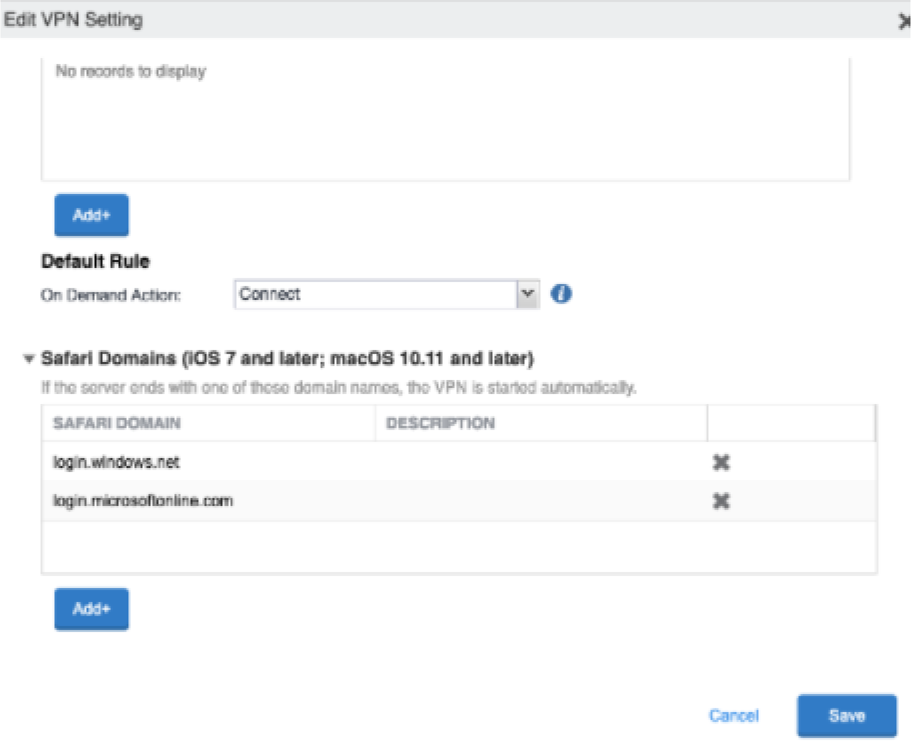
   b. Create a local Scep using local CA.

   c. Under **Add**, select VPN from the drop-down .

   d. Configure the following fields on **Add VPN Setting** window.

      - **Connection Type**: MobileIron Tunnel
      - **Sentry** - Select the second Sentry from the drop-down.
      - **Sentry service**: TCP
      - **Provider type**: App Proxy
      - **Identity certificate**: Local Scep from drop-down.
      - Open Safari domain section, add the following MS domains:
        - login.windows.net
        - login.microsoftonline.com
      - Save the settings and apply the label.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.



Edit VPN Setting

No records to display

Default Rule

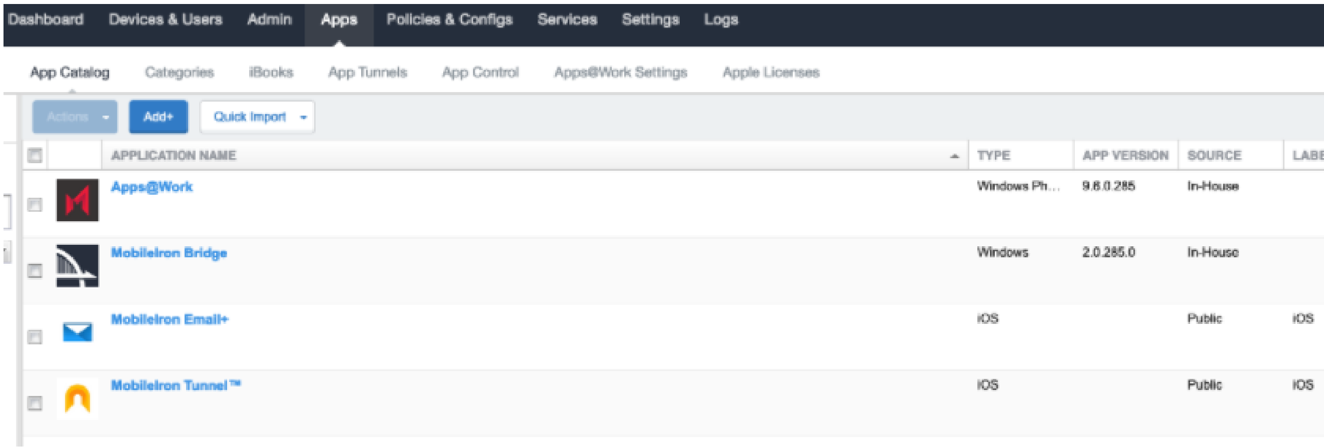
On Demand Action: Connect

Safari Domains (iOS 7 and later; macOS 10.11 and later)

If the server ends with one of these domain names, the VPN is started automatically.

SAFARI DOMAIN	DESCRIPTION	
login.windows.net		✖
login.microsoftonline.com		✖

3. Configure Ivanti Tunnel application in **Apps** > **App Catalog**.



	APPLICATION NAME	TYPE	APP VERSION	SOURCE	LABE
□	Apps@Work	Windows Ph...	9.8.0.285	In-House	
□	MobileIron Bridge	Windows	2.0.285.0	In-House	
□	MobileIron Email+	iOS		Public	iOS
□	MobileIron Tunnel™	iOS		Public	iOS

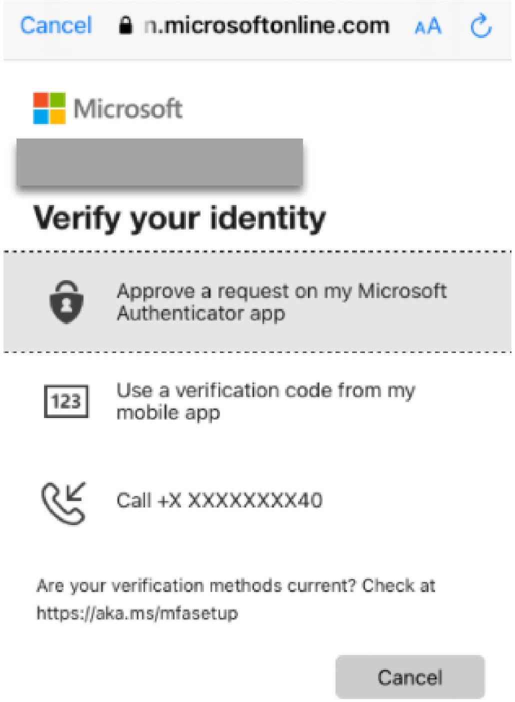
4. Register the device with Office 365 user and complete the MDM enrollment.

5. Download Ivanti Tunnel application from Apps@work and complete the device registration.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

6. Launch Native mail application and click on **Edit settings** option.
   The user is now redirected to Microsoft online to enter the password.

7. Enter the password.
   The user is now prompted for MFA on the device.



[redacted]

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

Call +X XXXXXXXX40

Are your verification methods current? Check at https://aka.ms/mfasetup

8. After selecting MFA option, authentication is successful and user is redirected back to the mailbox.

Configuring OAuth for Android Email+ on Ivanti EPMM

Before you begin

- Verify that you use Office 365 and have an Office 365 certificate.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. On Core, click Policies and **Configs** > **Configurations** > **Add New** > **Certificate Enrollment** > **Single File Identity**.

2. Add the **Office 365 certificate**.

3. On Core, click **Apps** and perform the following steps:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

a. Select **Google Play** and search for Ivanti Email+ application.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

b. Under App Configurations, select Email+ application:

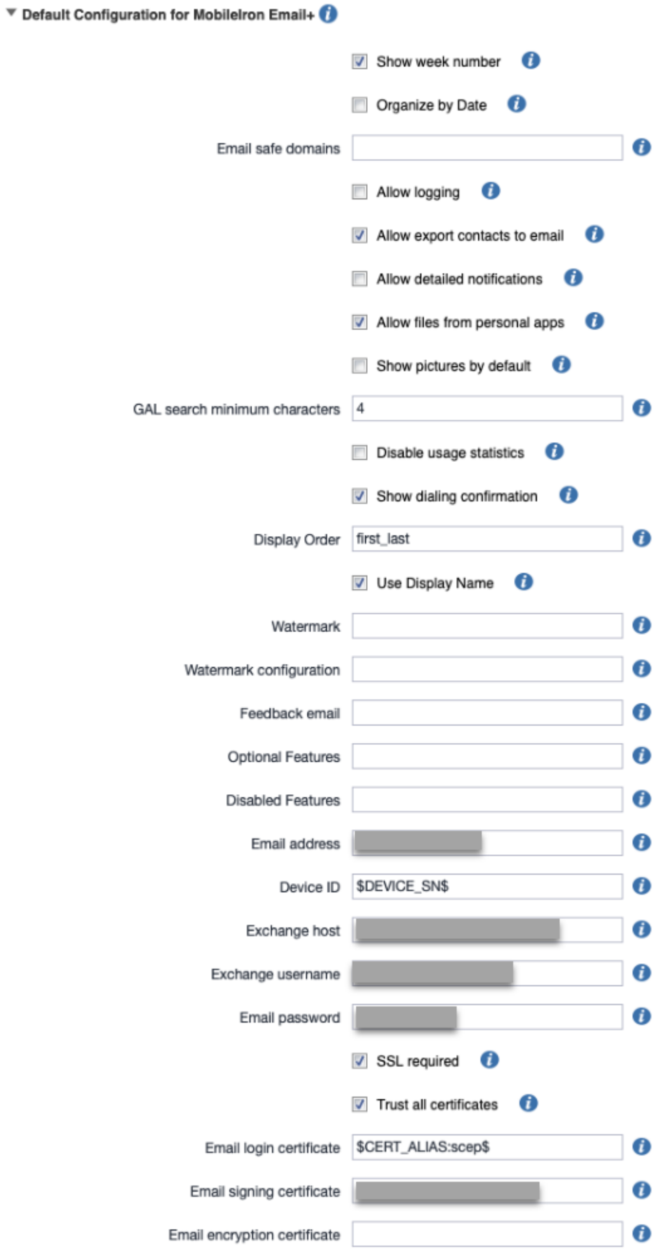
  - Enable **Install this App for Android Enterprise**.
  - Under **Configuration** choices, select the default configuration :
    - Configure Email address
    - Device ID
    - Exchange host: Sentry 1 server hostname
    - Exchange username
    - Email Password
    - Enable SSL required and Trust all Certificate options
    - Configure email login certificate
    - Configure email signing certificate

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Select **Authorization mode**
  - **Authorization mode**: Modern Authentication
  - **EWS Authentication mode**: Basic Authentication
  - Configure Modern Auth Authority URL

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Configure Modern Auth resource URL



▼ **Default Configuration for MobileIron Email+**

☑ Show week number

□ Organize by Date

Email safe domains:

□ Allow logging

☑ Allow export contacts to email

□ Allow detailed notifications

☑ Allow files from personal apps

□ Show pictures by default

GAL search minimum characters: 4

□ Disable usage statistics

☑ Show dialing confirmation

Display Order: first_last

☑ Use Display Name

Watermark:

Watermark configuration:

Feedback email:

Optional Features:

Disabled Features:

Email address: [redacted]

Device ID: $DEVICE_SN$

Exchange host: [redacted]

Exchange username: [redacted]

Email password: [redacted]

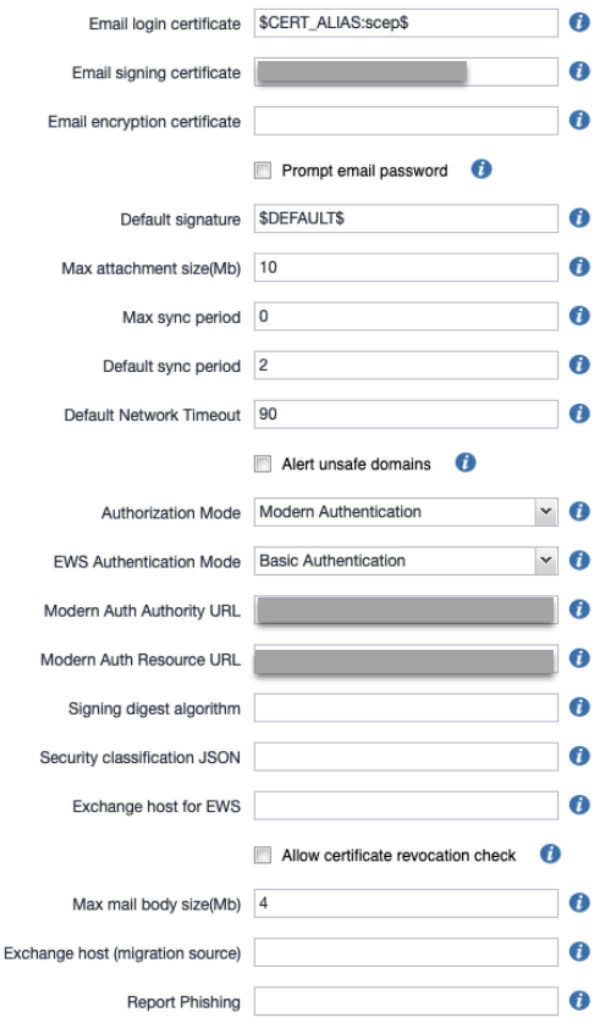
☑ SSL required

☑ Trust all certificates

Email login certificate: $CERT_ALIAS:scep$

Email signing certificate: [redacted]

Email encryption certificate:



Email login certificate	$CERT_ALIAS:scep$
Email signing certificate	[redacted]
Email encryption certificate	
	□ Prompt email password
Default signature	$DEFAULT$
Max attachment size(Mb)	10
Max sync period	0
Default sync period	2
Default Network Timeout	90
	□ Alert unsafe domains
Authorization Mode	Modern Authentication
EWS Authentication Mode	Basic Authentication
Modern Auth Authority URL	[redacted]
Modern Auth Resource URL	[redacted]
Signing digest algorithm	
Security classification JSON	
Exchange host for EWS	
	□ Allow certificate revocation check
Max mail body size(Mb)	4
Exchange host (migration source)	
Report Phishing	

- Apply the configuration and click **Finish**.
- Register the device with MDM and install **Android Enterprise Work Profile**.
- Install **Tunnel**and **Email+**
- Download Tunnel application.
- Launch Email+ application and authenticate.
- Enter the password to authenticate.
  The user is now prompted for MFA on the device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configuring OAuth for Android Enterprise Email+ on Ivanti EPMM

1. On the first Sentry, configure OAuth. See "OAuth for Sentry on Ivanti EPMM" on page 69.

2. Configure another Sentry hostname on Tunnel application and complete the following steps on Ivanti EPMM:

a. On **Ivanti EPMM**, click **Apps**.

b. Click **Add** > **Google Play** > select **Ivanti Tunnel**.

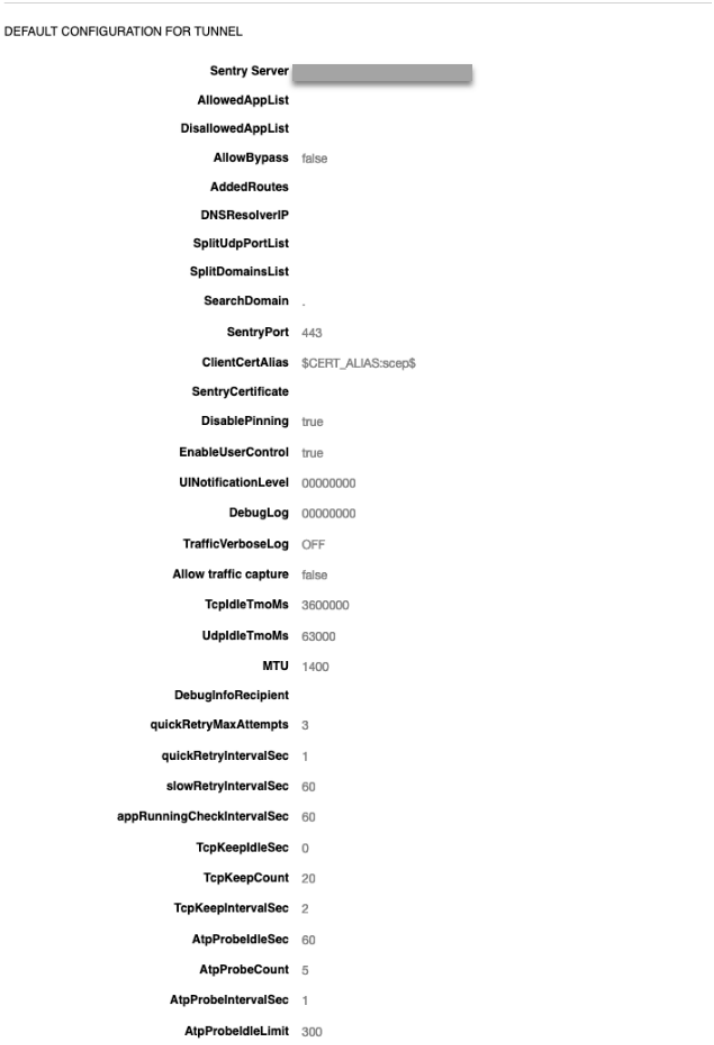
c. Enable **Install this app for Android Enterprise**.

d. Configure Sentry server hostname as Sentry 2.

e. Configure **Client CertAlias**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

f. Save the configuration and apply the labels.



DEFAULT CONFIGURATION FOR TUNNEL

Sentry Server	[redacted]
AllowedAppList	
DisallowedAppList	
AllowBypass	false
AddedRoutes	
DNSResolverIP	
SplitUdpPortList	
SplitDomainsList	
SearchDomain	.
SentryPort	443
ClientCertAlias	$CERT_ALIAS:scep$
SentryCertificate	
DisablePinning	true
EnableUserControl	true
UINotificationLevel	00000000
DebugLog	00000000
TrafficVerboseLog	OFF
Allow traffic capture	false
TcpIdleTmoMs	3600000
UdpIdleTmoMs	63000
MTU	1400
DebugInfoRecipient	
quickRetryMaxAttempts	3
quickRetryIntervalSec	1
slowRetryIntervalSec	60
appRunningCheckIntervalSec	60
TcpKeepIdleSec	0
TcpKeepCount	20
TcpKeepIntervalSec	2
AtpProbeIdleSec	60
AtpProbeCount	5
AtpProbeIntervalSec	1
AtpProbeIdleLimit	300

Configuring OAuth for iOS Email+ on Ivanti EPMM

Before you begin

- Verify that you have a second Sentry with appconfig.

Procedure

1. On the first Sentry, configure OAuth. See "OAuth for Sentry on Ivanti EPMM" on page 69.

2. On the second Sentry, configure Email+ for iOS.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- On **Ivanti EPMM**, click **Services** > **Sentry** > **Add new Sentry**.
- On Sentry configuration, update the following fields:

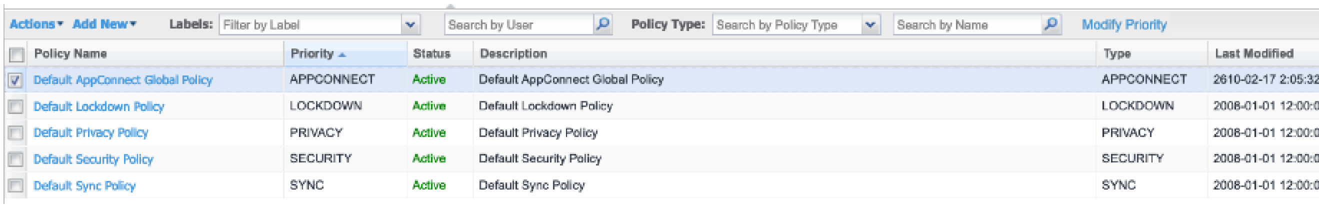
  a. Enable **App Tunnel**.

  b. Upload **Identity Certificate** (local CA) for Device Authentication.

  c. Under Services, click **Configure ANY service**.

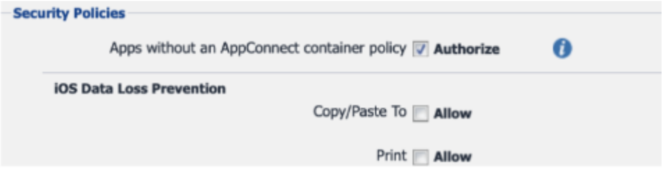
  d. Save **Sentry settings**.

- Click **Policies and Config** and update the following:
- Click **Policies** and select **Default App Connect global policy**.



☐	Policy Name	Priority ▲	Status	Description	Type	Last Modified
☑	Default AppConnect Global Policy	APPCONNECT	Active	Default AppConnect Global Policy	APPCONNECT	2610-02-17 2:05:32
☐	Default Lockdown Policy	LOCKDOWN	Active	Default Lockdown Policy	LOCKDOWN	2008-01-01 12:00:0
☐	Default Privacy Policy	PRIVACY	Active	Default Privacy Policy	PRIVACY	2008-01-01 12:00:0
☐	Default Security Policy	SECURITY	Active	Default Security Policy	SECURITY	2008-01-01 12:00:0
☐	Default Sync Policy	SYNC	Active	Default Sync Policy	SYNC	2008-01-01 12:00:0

- Edit the policy and enable **App Connect**.
- Enable **Authorize** security policy and save the settings.



Security Policies

Apps without an AppConnect container policy ☑ Authorize

iOS Data Loss Prevention

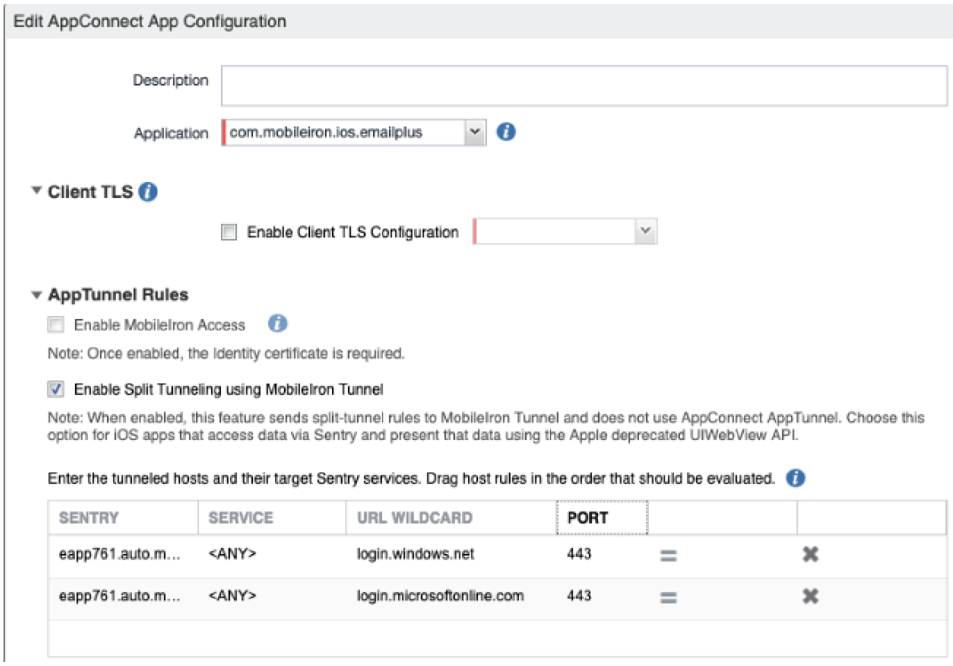
Copy/Paste To ☐ Allow

Print ☐ Allow

- Click **Policies and Config** and select **Configuration**. Update the following:
- In **Add New**, select **AppConnect** > **App Configuration**.
- Configure **Application Bundle ID for Email+**.
- Enable **Split Tunnel rules**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Under Tunneled hosts and configured services:
  - Add Sentry 2 from the drop-down.
  - Select **Any Service**.
  - **URL wildcard**: login.windows.net
    - **Port**: 443
    - Add another Sentry and select the Sentry and Service Name same as above.
  - **URL wildcard**: login.microsoftonline.com
    - **Port**: 443



Edit AppConnect App Configuration

Description:

Application: com.mobileiron.ios.emailplus

Client TLS

□ Enable Client TLS Configuration

AppTunnel Rules

□ Enable MobileIron Access

Note: Once enabled, the Identity certificate is required.

☑ Enable Split Tunneling using MobileIron Tunnel

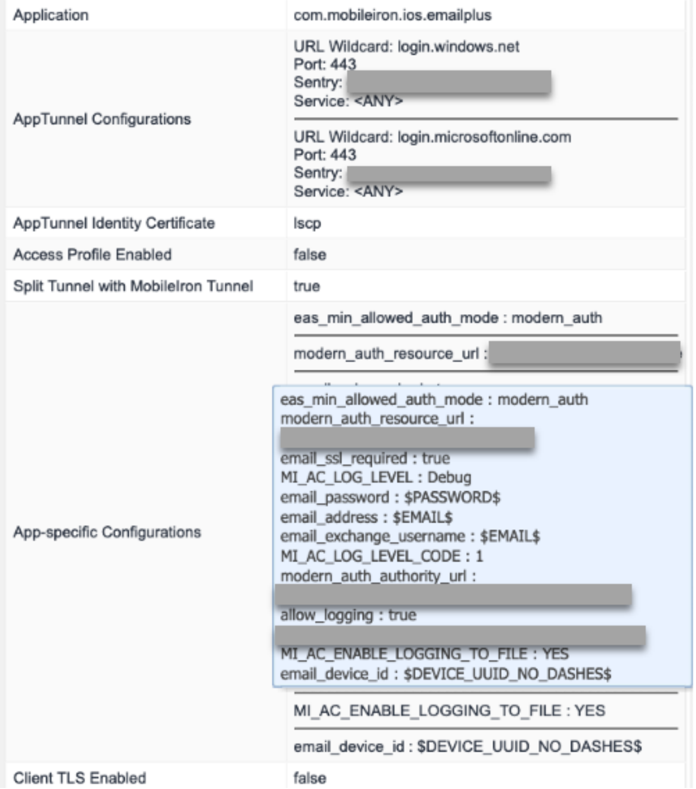
Note: When enabled, this feature sends split-tunnel rules to MobileIron Tunnel and does not use AppConnect AppTunnel. Choose this option for iOS apps that access data via Sentry and present that data using the Apple deprecated UIWebView API.

Enter the tunneled hosts and their target Sentry services. Drag host rules in the order that should be evaluated.

SENTRY	SERVICE	URL WILDCARD	PORT		
eapp761.auto.m...	<ANY>	login.windows.net	443	=	✖
eapp761.auto.m...	<ANY>	login.microsoftonline.com	443	=	✖

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configure **Email+KVPs** under App specific configurations:



Application	com.mobileiron.ios.emailplus
AppTunnel Configurations	URL Wildcard: login.windows.net Port: 443 Sentry: [redacted] Service: <ANY> URL Wildcard: login.microsoftonline.com Port: 443 Sentry: [redacted] Service: <ANY>
AppTunnel Identity Certificate	lscp
Access Profile Enabled	false
Split Tunnel with MobileIron Tunnel	true
App-specific Configurations	eas_min_allowed_auth_mode : modern_auth modern_auth_resource_url : [redacted] MI_AC_ENABLE_LOGGING_TO_FILE : YES email_device_id : $DEVICE_UUID_NO_DASHES$
Client TLS Enabled	false

eas_min_allowed_auth_mode : modern_auth
modern_auth_resource_url :
[redacted]
email_ssl_required : true
MI_AC_LOG_LEVEL : Debug
email_password : $PASSWORD$
email_address : $EMAIL$
email_exchange_username : $EMAIL$
MI_AC_LOG_LEVEL_CODE : 1
modern_auth_authority_url :
[redacted]
allow_logging : true
[redacted]
MI_AC_ENABLE_LOGGING_TO_FILE : YES
email_device_id : $DEVICE_UUID_NO_DASHES$

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry for AppTunnel

The following describe how to configure Ivanti Standalone Sentry for AppTunnel:

Overview of configuring Ivanti Standalone Sentry for AppTunnel

Ivanti Standalone Sentry configured for AppTunnel provides device users secure access to your company's backend resource such as a SharePoint server.

You configure Ivanti Standalone Sentry for AppTunnel in the Ivanti EPMM Admin Portal. AppTunnel is part of Ivanti Tunnel deployment or an AppConnect app deployment.

To setup secure access to backend resources:

1. In the Ivanti EPMM Admin Portal configure a Ivanti Standalone Sentry for AppTunnel.
2. Configure one of the following for apps:
   - Configure an AppConnect app.

   Or
   - Configure Ivanti Tunnel.

Configuring Ivanti Standalone Sentry for AppTunnel

If you configure AppTunnel on a Ivanti 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.

Before you begin

1. You must have installed Standalone Sentry. See the *Ivanti Standalone Sentry Installation Guide*.
2. Ensure that you have the required certificate setup in your UEM. AppTunnel uses either an Identity certificate or Kerberos for device authentication.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Admin Portal, go to Services > Sentry.
2. Select **Add New > Standalone Sentry** or click the **Edit** icon for an existing Standalone Sentry entry.
3. Complete the fields to configure Standalone Sentry for AppTunnel.
4. Click **Save**.
5. Perform these steps if the Standalone Sentry uses a third-party certificate:

    - Go to **Services > Sentry.**

    - For the Sentry configured for app tunneling, click the **View Certificate** link.

This makes the certificate for Sentry known to Ivanti EPMM.

ⓘ Ivanti Standalone Sentry displays a warning message when customers attempt to generate and use a self-signed certificate for a TLS handshake between Sentry and Tunnel.

Related topics

- See the following section to complete the fields in the Standalone Sentry form for configuring ActiveSync:

- "Ivanti Standalone Sentry connectivity settings" below
- "Enable AppTunnel" on the next page
- "Device authentication" on the next page
- "Context headers" on the next page
- "Enable DFS" on page 96
- "Advanced Traffic Control and server-side explicit proxy" on page 97
- "AppTunnel service" on page 102
- "Configured settings for managing multiple Sentrys" on page 107
- "Advanced settings" on page 108

- See "Configure apps" on page 108 for information about configuring AppConnect apps or for configuring Ivanti Tunnel.

Ivanti Standalone Sentry connectivity settings

The following table describes the fields for configuring the connectivity settings for Ivanti Standalone Sentry.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 12. IVANTI STANDALONE SENTRY CONNECTIVITY SETTINGS

Item	Description
Sentry Host / IP	Enter the host name or IP address of the server on which the Ivanti Standalone Sentry is installed.
Sentry Port	Enter the port that Ivanti EPMM will use to access the Ivanti Standalone Sentry. The default is 9090.

Enable AppTunnel

In the Ivanti Standalone Sentry form, select **Enable AppTunnel**. The AppTunnel Configuration section displays.

Device authentication

The Device Authentication setting, in the Ivanti Standalone Sentry form, determines how users attempting to connect to the ActiveSync server or backend resource authenticate with Ivanti Standalone Sentry.

See "Device and Server Authentication" on page 109 for information on selecting and configuring a method of device authentication.

See "Multiple trusted root certificates for device authentication" on page 122 for information on uploading multiple trusted root certificates for device authentication.

Context headers

As an administrator you may require your corporate backend resources to further validate the devices accessing the resources. In these cases, Ivanti Standalone Sentry forwards context information in the header. Context headers is a global setting. It is applied to all services except ActiveSync. Context headers will be added to all HTTP requests, including HTTP tunnels and IP tunnels. Context Headers will also be added to the CONNECT requests for TCP Tunnel and non-HTTP requests sent through IP tunnels.

Context Headers are supported primarily for HTTP Tunnels. However for TCP & IP Tunnels, context headers are supported for the following cases:

- HTTP traffic (port 80)
- HTTP CONNECT request when explicit proxy is configured

The following table describes the context information available in headers.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 13. CONTEXT INFORMATION IN HEADERS

Header Name	Description
X-MobileIron-DEVICE-UUID	Device UUID The Device UUID can be used in API calls to Ivanti EPMM to collect more information about the device.
X-MobileIron-USER-UPN	User Principal name
X-MobileIron-USER-DN	User DN (if available)
X-MobileIron-USER-CERT	User Identity certificate The certificate is represented in a Privacy Enhanced Mail (PEM) encoding without the header or the trailer information.

The following table describes the field for enabling context headers.

TABLE 14. FIELD DESCRIPTION FOR CONTEXT HEADERS

Item	Description
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 If server-side explicit proxy is configured, the request to the proxy (HTTP CONNECT) includes the context headers.

Enable DFS

The following provides a description of the field for enabling DFS.

TABLE 15. FIELD DESCRIPTION FOR ENABLE DFS

Item	Description
Enable DFS	Select the check box if you are configuring a DFS site in Docs@Work. See the *Docs@Work Guide* for information on how to set up a DFS site in Docs@Work.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Advanced Traffic Control and server-side explicit proxy

Standalone Sentry supports advanced traffic control (ATC) and server-side explicit proxy. The following describe the support:

- "Advanced traffic control (ATC)" below
    - "Server-side explicit proxy" below
    - "Field descriptions for configuring ATC and server-side proxy" on page 99

Advanced traffic control (ATC)

Advance traffic control (ATC) allows you to manage access to backend resources based on which app the traffic is coming from, OS platform, 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 Ivanti Standalone Sentry version 7.0.1 or earlier, and configure ATC rule for a specific app on Ivanti EPMM, Ivanti Standalone Sentry will ignore the rule.

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 Sentry and corporate resources. This deployment allows you to access corporate resources without having to open the ports that Sentry would otherwise require.

- 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.

Ivanti 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, Ivanti Standalone Sentry will treat the explicit proxy as HTTP proxy. The HTTP request URL will be modified to include the target host.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

In all other cases, Ivanti 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.

Traffic control rules

Traffic control rules specify whether traffic from an AppTunnel service or Ivanti Tunnel to the backend resource is through a proxy server, allowed direct access, or blocked. Traffic control rules are applied to the following **Services**:

- custom name
- ANY
- TCP_ANY
- IP_ANY

Rules 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.

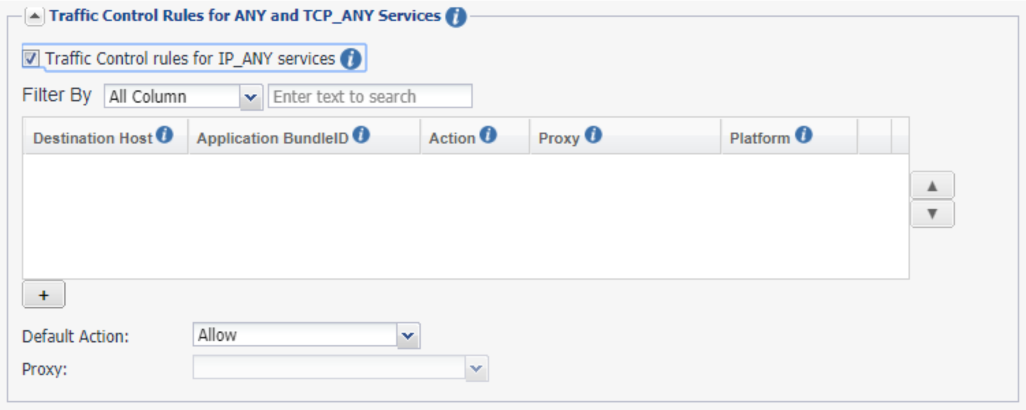
- If AppTunnel traffic is blocked due to traffic control rules, the AppTunnel entry is not reported in the **Apps > AppTunnels** page in the Admin Portal.
- To enable the traffic control rules for ANY and TCP_ANY services, you must select the <ANY> or <TCP_ANY> checkbox in the **Proxy/ATC** column of **Services** panel. See, "AppTunnel service" on page 102.
- To enable the traffic control rules for IP_ANY services, you must select <IP_ANY> checkbox in the **Proxy/ATC** column of **Services** panel. See, "AppTunnel service" on page 102.

Traffic control rules for ANY and TCP_ANY services

Sentry parses custom, ANY, TCP_ANY service traffic for the destination host and the application ID. For HTTP traffic Sentry obtains the information from the host address. For HTTPS traffic Sentry obtains the information from the SNI. The information is used to match against domain-based ATC rules. If the information is not available or the information does not match a rule, the default rule is applied.

If the option **Traffic Control rules for IP_ANY services** is enabled, Sentry parses and obtains the destination host and application ID and applies the domain-based ATC rules. If Sentry cannot get the destination host and application ID information, then IP-based ATC rules are applied.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.



Traffic Control Rules for ANY and TCP_ANY Services

☑ Traffic Control rules for IP_ANY services

Filter By: All Column — Enter text to search

Destination Host	Application BundleID	Action	Proxy	Platform

Default Action: Allow

Proxy:

Traffic control rules for IP_ANY Service

Sentry uses the destination IP address for IP_ANY service traffic to match against an IP-based ATC rule. If the information is not available or the information does not match a rule, the default rule is applied.

Field descriptions for configuring ATC and server-side proxy

The following table describes the fields for configuring ATC and server-side proxy.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 16. FIELD DESCRIPTIONS FOR ADVANCED TRAFFIC CONTROL (ATC)

Item	Description
Advanced Traffic Control	Select the checkbox to enable advanced traffic control. The **Server-side Proxy** section is replaced with the **Advanced Traffic Control (ATC)** section.
Server-side Proxy List Traffic is directed to the proxy servers listed here based on the backend resource and action defined in **Traffic Control Rules.**	
Name	Enter a unique name for the proxy server. The name for the proxy server will be available for selection in the **Proxy** field.
Hostname	Enter the IP address or FQDN for the proxy server.
Port	Enter the port number for the proxy server.
+	Click to add a proxy server.
Traffic control rules for ANY and TCP_ANY Services	
Traffic control rules for IP_ ANY services	Select the check box to configure Destination Host, Application BundleID, and device Platform for IP_ANY services. This triggers the rules under ANY and TCP_ANY services. Configure an ATC rule using FQDN for the destination host and specify a bundle ID. Specify the device OS to which the ATC rule is applied.
Search	Enter the text to search for the appropriate ATC rule or host based on domain, app identifier or other parameters listed in the ATC.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 16. FIELD DESCRIPTIONS FOR ADVANCED TRAFFIC CONTROL (ATC) (CONT.)

Item	Description
Destination Host	**IP address or domain name:** Enter the IP address or domain name of the backend resource: Port numbers are not supported. Wildcards are supported. Only the suffix after the * wildcard is matched. Example: *.acme.com. **ANY_SHORT:** Select **ANY_SHORT** to apply the traffic control rule to all short domain names entered by the device user. Example: The device user can enter sharepoint1 instead of sharepoint1.mycompany.com. Traffic control rules are applied to sharepoint1. **ANY_IP:** Select **ANY_IP** to apply traffic control rules to all IP addresses entered by the device user. Example: A device user entering an IP address to access example.mycompany.com can bypass a traffic control rule that directs traffic to *.mycompany.com through a proxy server. If you set traffic control rules to block **ANY _IP**, then traffic using the IP address is blocked.
Application Bundle ID	Enter the app identifier. The app identifier is the bundle ID for iOS apps and the package name for Android apps. The ID can include "*" for wildcard matching. The ID can be used in conjunction with Destination Host. If you are using the ID with a destination host, then the rule will be applied only to traffic from the app directed to the destination host.
Platform	You can also filter based on **Platform** such as iOS, macOS and Android. Windows is not supported.
Traffic control rules for IP_ANY Services	
Destination IP Address / CIDR	**IP address:** Enter the IP address or the CIDR notation of the backend resource.
Common field description for ANY, TCP_ANY, and IP_ANY Services	
Action	Select **Proxy**, **Allow**, or **Block**.
Proxy	If you selected **Proxy** for **Action**, then select the proxy server for the backend resource.
+	Click to add a backend resource.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 16. FIELD DESCRIPTIONS FOR ADVANCED TRAFFIC CONTROL (ATC) (CONT.)

Item	Description
Default Action	The default action is applied if traffic control rules is not defined for a backend resource.
Proxy	If you choose **Proxy** as the default action, select the proxy server for traffic to the backend resource.
Server-side Proxy If **Advanced Traffic Control (ATC)** is enabled, the Server-side Proxy section is no longer available. If you had configured a proxy server, and you enable advanced traffic control, the proxy server is listed in the **Server-side Proxy List** as global. The **Default Action** is selected as Proxy and the default **Proxy** server is selected as global. To configure Server-side Proxy, enter the HTTP proxy server information. Configuring an HTTP proxy server provides access to corporate resources without having to open the ports that Standalone Sentry would otherwise require.	
Proxy Host Name / IP	Enter the FQDN of the proxy server. Do not include a URI scheme, such as http:// or https://, in this field.
Proxy Port	Enter the port number for the proxy server.

AppTunnel service

The following table describes the fields for configuring an AppTunnel service.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 17. FIELD DESCRIPTIONS FOR APPTUNNEL SERVICE

Item	Description
Services To add a new AppTunnel service, click +.	
Service Name	The **Service Name** 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 **Server List** field. The service name is similarly used in: • the Web@Work setting for configuring tunneling for Web@Work for Android or iOS. • the Docs@Work setting for configuring tunneling for the Docs@Work app. The order of the **Service Name** entries does not matter. A service name cannot contain these characters: 'space' \ ; * ? < > " |. Enter one of the following: • A unique name for the service that the app on the device accesses. For example, some possible service names are: - SharePoint - Human Resources • A unique name with one of the following special prefixes: - For app tunnels that point to CIFS-based content servers, the service name must begin with **CIFS_**. - For TCP tunneling, the name must begin with **TCP** (case-insensitive). Example: **TCP_Finance**

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 17. FIELD DESCRIPTIONS FOR APPTUNNEL SERVICE (CONT.)

Item	Description
Service Name	- **<ANY>** Select **<ANY>** to allow tunneling to any URL that the app requests. Typically, you select **<ANY>** if an AppConnect app's app configuration specifies a URL with wildcards for tunneling, such as *.myCompany.com. Sentry tunnels the data for any URL request that the app makes that matches the URL with wildcards. Sentry tunnels the data to the backend resource that has the URL that the app specified. The **Server List** field is therefore not applicable when the Service Name is **<ANY>**. For example, consider when the app requests URL myAppServer.mycompany.com, which matches *.mycompany.com in the app configuration. Sentry tunnels the data to myAppServer.myCompany.com. Web@Work typically uses the **<ANY>** service, so that it can browse to any of your internal servers. Do not select this option for tunneling to CIFS-based content servers. Select **<CIFS_ANY>** instead.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 17. FIELD DESCRIPTIONS FOR APPTUNNEL SERVICE (CONT.)

Item	Description
Service Name	• **<TCP_ANY>**. Select **<TCP_ANY>** to allow TCP tunneling to any backend resource that the app requests. • **<CIFS_ANY>** Select **<CIFS_ANY>** to allow tunneling to any URL for a CIFS-based content server. Typically, you select **<CIFS_ANY>** if the URL for a CIFS-based content server contains wildcards for tunneling, such as *.myCompany.com. • **<IP_ANY>** Select **<IP_ANY>** to allow IP tunneling. Use this service name as part of the Ivanti Tunnel setup for Windows 10 or Android devices. By default, Sentry uses 172.28.13.0/29 as the subnet mask for IP tunnels. If you are using the subnet internally, you must change the subnet Sentry uses. Contact Support for instructions on how to change the default subnet mask that Standalone Sentry uses for IP tunneling. • **<IP_ANY_WP8.1>** Select **<IP_ANY_WP8.1>** to allow IP tunneling for WP8.1 devices. Use this service name as part of the Tunnel setup for Windows Phone 8.1 (WP8.1) devices.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 17. FIELD DESCRIPTIONS FOR APPTUNNEL SERVICE (CONT.)

Item	Description
Server Auth	Select the authentication scheme for the Standalone Sentry to use to authenticate the user to the backend resource: • **Pass Through** Sentry passes through the authentication credentials, such as the user ID and password (basic authentication) or NTLM, to the backend resource. For TCP and IP tunneling, select Pass Through. Pass Through is the only option available when the service name begins with “TCP”. Sentry passes through all TCP or IP packets to the backend resource. • **Kerberos** 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. The **Kerberos** option is only available if: - You selected **Identity Certificate** for **Device Authentication**. - The service name is not a TCP service name; Ivanti, Inc does not support Kerberos for AppTunnel with TCP tunneling.
Server List	Enter the backend resource’s host name or IP address (usually an internal host name or IP address). Include the port number on the backend resource that 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. Standalone 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. Separate each resource name with a semicolon. Example: sharepoint1.companyname.com:443;sharepoint2.companyname.com:443. The Server List field is not applicable when the service name is **<ANY>**, **<TCP_ANY>**, **<IP_ANY>,** or **<CIFS_ANY>**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 17. FIELD DESCRIPTIONS FOR APPTUNNEL SERVICE (CONT.)

Item	Description
TLS Enabled	Select **TLS Enabled** if the servers listed in the **Server List** field require SSL. This option is not applicable when the service name is **<ANY>**, **<TCP_ANY>**, **<CIFS_ANY>**, **<IP_ANY>**, or a TCP service. ⓘ Although port 443 is typically used for https and requires SSL, the backend resource can use other port numbers requiring SSL.
Proxy/ATC	Select if you want to direct the AppTunnel service traffic through the proxy server. You must also have configured **Server-side Proxy** or **Advanced Traffic Control (ATC)**.
Server SPN List	Enter the Service Principal Name (SPN) for each server, separated by semicolons. Example: sharepoint1.company.com;sharepoint2.company.com. The **Server SPN List** applies only when the Service Name is not **<ANY>** and the **Server Auth** is Kerberos. If each server in the **Server List** has the same name as its SPN, you can leave the **Server SPN List** empty. However, if you include a **Server SPN List**, the number of SPNs listed must equal the number of servers listed in the **Server List**. The first server in the **Server List** corresponds to the first SPN in the **Server SPN List**, the second server in the **Server List** corresponds to the second server in the **Server SPN List**, and so on. For a custom CIFS AppTunnel service, if you configured the FQDN of the CIFS server in the server list, and the FQDN is the same as the SPN, you do not need to configure the **Server SPN List**. A custom CIFS service is an AppTunnel service that is not CIFS_ANY. If you configured the IP address of the CIFS server in the server list, you must configure the corresponding SPN. The SPN must include the cifs prefix. Example: cifs/s01-dfs12-001.example.com. Any SPN configured for a CIFS service must inlcude the cifs prefix. ⓘ When the **Service Name** is **<ANY>** and the **Server Auth** is **Kerberos**, the Standalone Sentry assumes that the SPN is the same as the server name received from the device. This field is not applicable for a TCP service.

Configured settings for managing multiple Sentrys

See "Configured settings for managing multiple servers" on page 44.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Advanced settings

See "Advanced settings" on page 45.

Configure apps

After configuring AppTunnel on Ivanti Standalone Sentry, you must configure the apps to use AppTunnel. See the app's documentation for information on how to set up the app.

TABLE 18. REFERENCE TO APP DOCUMENTATION

App	Documentation
Ivanti Tunnel	Ivanti Tunnel for iOS and macOS documentation Ivanti Tunnel for Windows documentation Ivanti Tunnel for Android documentation
AppConnect apps	*Ivanti EPMM AppConnect and AppTunnel Guide*
Docs@Work	Ivanti Docs@Work for iOS Ivanti Docs@Work for Android
Email+	Ivanti Email+ for iOS Ivanti Email+ for Android
Web@Work	Web@Work for iOS Web@Work for Android

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Device and Server Authentication

The following describe the options and configuration for device and server authentication on Ivanti Standalone Sentry:

Overview of device and server authentication with Ivanti Standalone Sentry

Ivanti 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 Ivanti Standalone Sentry)

See "Device authentication configuration on Ivanti Standalone Sentry" below.

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

See "Server authentication on Ivanti Standalone Sentry" on page 111.

Device authentication configuration on Ivanti Standalone Sentry

Device authentication specifies how the device authenticates to the Ivanti Standalone Sentry. The following table describes the device authentication options on Ivanti Standalone Sentry.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Table 19. Types of device authentication supported in Standalone Sentry

Device Authentication	Description
Pass Through	Only available if you are using Sentry for ActiveSync only. Sentry passes through the following authentication provided by the device: user name and password or NTLM.
Group Certificate	Available for ActiveSync and AppTunnel. Requires the following: • A trusted group certificate for device authentication. • A authentication method like user name and password or NTLM for authenticating the device to the server. ⓘ KCD is not supported with Group Certificates.
Identity Certificate	Available for ActiveSync and AppTunnel. Requires the following: • A certificate issued by a Trusted Root Authority for device authentication. • A user name and password or a properly configured Kerberos implementation for authenticating the device to the server.
Trusted Front-End	Available for ActiveSync and AppTunnel. Requires the following: • Setting up an Apache or F5 proxy to front-end the Standalone Sentry. • Additional minor changes to references to the hostname in some profiles. ⓘ Ivanti supports only Apache or F5 servers as the trusted front-end server for TCP tunneling.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Server authentication on Ivanti Standalone Sentry

Server authentication specifies how Sentry authenticates the device to the backend resource. This can be the ActiveSync server or a backend resource.

Ivanti Standalone Sentry supports pass through or Kerberos for server authentication. These are supported for both ActiveSync and AppTunnel.

The following table describes the device authentication options on Ivanti Standalone Sentry.

TABLE 20. TYPES OF SERVER AUTHENTICATION SUPPORTED IN IVANTI STANDALONE SENTRY

Server Authentication	Description
Pass Through	Sentry passes through the authentication provided by the device. For example: user name and password, NTLM. 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.
Kerberos	Only available if you choose Identity Certificate for device authentication. Requires a properly configured Kerberos implementation.

Configuring device and server authentication

You specify the device and server authentication in the Sentry configuration under Services > Sentry in the Admin Portal. Click **Add New > Standalone Sentry** or click the **Edit** icon for an existing Sentry.

- Device authentication is configured in the Device Authentication Configuration section.
- Server authentication is configured:

- in the ActiveSync Configuration section for the ActiveSync server.
- in the App Tunneling Configuration section for each AppTunnel service.

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

For identity certificates, you can upload a local CA or an external CA. See the “Managing Certificates and Configuring Certificate Authorities” chapter in the Ivanti EPMM Device Management Guide for information on how to create a local CA, generate a certificate signing request (CSR), and configure Certificate and Certificate Enrollment settings.

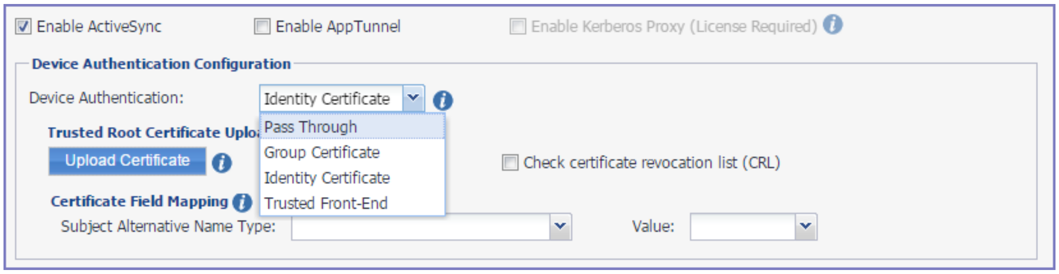
Before you begin

- Obtain the certificates required for your implementation.

Procedure

1. In the Admin Portal, select **Services** > **Sentry**.
2. Click the **Edit** icon the Standalone Sentry entry.

FIGURE 1. DEVICE AUTHENTICATION



☑ Enable ActiveSync □ Enable AppTunnel □ Enable Kerberos Proxy (License Required)

Device Authentication Configuration

Device Authentication: Identity Certificate

□ Check certificate revocation list (CRL)

Subject Alternative Name Type:

Value:

3. In the **Device Authentication Configuration** section, select an option appropriate for your implementation.
4. Depending on the option you selected, follow the instructions in one of the following section to complete the configuration:
   - **Pass Through**
   See "Configuring authentication using Pass Through" below for next steps.
   - **Group Certificate**
   See "Configuring authentication using a group certificate" on the next page for next steps.
   - **Identity Certificate**
   See "Configuring authentication using an identity certificate and Pass Through " on page 115 for next steps.
   OR
   See "Configuring authentication using an identity certificate and Kerberos constrained delegation" on page 116 for next steps.

Configuring authentication using Pass Through

With the pass through option, Ivanti Standalone Sentry passes through the user name and password or NTLM authentication provided by the device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Ivanti Standalone Sentry configuration on Ivanti EPMM, for **Device Authentication**, select **Pass Through**.

Pass Through is only option available for server authentication for the ActiveSync server.

2. Click **Save** to save your configuration.

Related topics

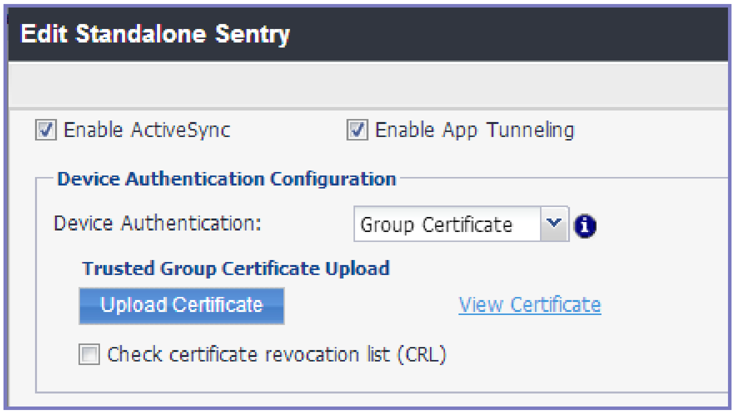
See also, "Device authentication configuration on Ivanti Standalone Sentry" on page 109

Configuring authentication using a group certificate

If you select **Group Certificate** for device authentication, additional configuration fields display in the **Device Authentication Configuration** section.

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

FIGURE 2. AUTHENTICATION USING GROUP CERTIFICATE



Edit Standalone Sentry

☑ Enable ActiveSync ☑ Enable App Tunneling

Device Authentication Configuration

Device Authentication: Group Certificate

Trusted Group Certificate Upload

Upload Certificate View Certificate

□ Check certificate revocation list (CRL)

Procedure

1. In the **Device Authentication Configuration** section
2. For **Device Authentication**, select **Group Certificate**.
3. Click **Upload Certificate**.
4. Select the certificate (usually a .cer file) you trust.
5. Click **Upload**.

The certificate is uploaded at this time, but 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)**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

  - 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. If you are configuring the Standalone Sentry for ActiveSync, in the ActiveSync Server Configuration section, **Server Authentication** defaults to **Pass Through**.

If you are configuring Standalone Sentry for AppTunnel, in the App Tunneling Configuration section, select **Pass Through** for **Server Auth** for the AppTunnel Service.

8. Click **Save**.

Ivanti Standalone Sentry restarts.

Next steps

Create a **Certificates** setting to generate the identity certificate for the device. Go to "Configuring a Certificates Enrollment setting" below.

Configuring a Certificates Enrollment setting

You will reference the certificate enrollment setting in the Exchange configuration if you are configuring ActiveSync email. If you are configuring AppTunnel, you will reference the certificate enrollment setting in the AppConnect app configuration, the Docs@Work configuration, or the Web@Work configuration, depending on the app for which you are configuring an AppTunnel service. The certificate is pushed to the device along with the configuration in which the certificate is referenced. You do not need to apply the certificate setting to a label.

Procedure

1. In the Admin Portal, go to **Policies & Configs** > **Configurations**.
2. Click **Add New** > **Certificate Enrollment** > **Single File Identity**.
3. Enter the requested information and upload the certificate.

This is the same certificate you uploaded for device authentication to the Ivanti Standalone Sentry. You will upload the certificate and the key (a .p12 file).

4. Click **Save**.

Related topics

For more information about the **Single File Identity** setting, see the Ivanti EPMM Device Management Guide.

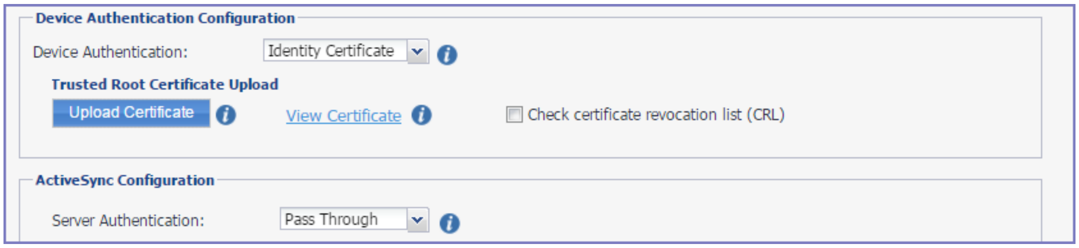
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configuring authentication using an identity certificate and Pass Through

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

If you select **Identity Certificate** for device authentication, additional configuration fields display in the **Device Authentication Configuration** section.

FIGURE 3. DEVICE AUTHENTICATION WITH IDENTITY CERTIFICATE



Device Authentication Configuration

Device Authentication: Identity Certificate

Trusted Root Certificate Upload

□ Check certificate revocation list (CRL)

ActiveSync Configuration

Server Authentication: Pass Through

Procedure

1. In the **Device Authentication Configuration** section, click **Upload Certificate**.
2. Select the Root certificate (this may be a root certificate chain) that you received from the CA you trust. The CA may be a Root Authority or an Intermediate Authority.
3. Click **Upload**.

The certificate is uploaded at this time, but does not persist until you click **Save**.

4. 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)**.

   - CRL check should be enabled only if the certificate chain presented by the device or the Trusted-Front-End to Ivanti 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.
5. If you are configuring Standalone Sentry for ActiveSync, in the **ActiveSync Server Configuration** section, **Server Authentication** defaults to **Pass Through**.

If you are configuring Standalone Sentry for AppTunnel, in the **App Tunneling Configuration** section, select **Pass Through** for **Server Auth** for the AppTunnel Service.

6. Click **Save**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Standalone Sentry restarts.

Next steps

Create a **Certificates Enrollment** setting to generate the identity certificate for the device. Go to "Configuring a Certificates Enrollment setting" below.

Configuring a Certificates Enrollment setting

You will reference the certificates enrollment setting in the Exchange configuration if you are configuring ActiveSync email. If you are configuring AppTunnel, you will reference the certificate enrollment setting in the AppConnect app configuration, the Docs@Work configuration, or the Web@Work configuration, depending on the app for which you are configuring an AppTunnel service. The certificate is pushed to the device along with the configuration in which the certificate is referenced. Do not apply the certificate setting to a label.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Click **Add New > Certificates Enrollment**.
3. Select and configure the appropriate certificate enrollment setting.

The identity certificate generated must be trusted by the certificate chain in the certificate you uploaded to the Ivanti Standalone Sentry for device authentication.

4. Click **Save**.

Next steps

For more information about **Certificate Enrollment** settings, see the Ivanti EPMM Device Management Guidefor your device operating system. For Android enterprise, see the Ivanti EPMM Device Management Guidefor Android.

Configuring authentication using an identity certificate and Kerberos constrained delegation

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

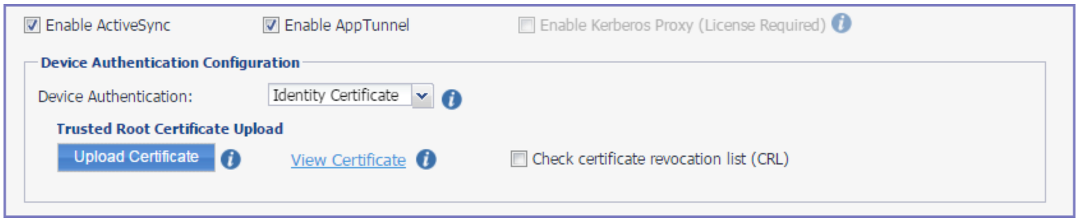
- For ActiveSync, Sentry supports Kerberos authentication only with Microsoft Exchange Servers.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- 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 127.
- Kerberos initialization in Standalone Sentry occurs only during tomcat start up. Ivanti Standalone Sentry obtains the ticket-granting ticket (TGT) during Kerberos initialization. If the initialization fails during tomcat start up, Ivanti 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. For more information on the debug command, see "Command Line Interface" on page 271.

If you select **Identity Certificate** for device authentication, additional configuration fields display in the Device Authentication Configuration section.

FIGURE 4. DEVICE AUTHENTICATION CONFIGURATION



☑ Enable ActiveSync ☑ Enable AppTunnel □ Enable Kerberos Proxy (License Required)

Device Authentication Configuration

Device Authentication: Identity Certificate

Trusted Root Certificate Upload

□ Check certificate revocation list (CRL)

Before you begin

Set up your environment. See *Authentication Using Kerberos Constrained Delegation* on the Support site.

Procedure

1. In the **Device Authentication Configuration** section:

Click **Upload Certificate**.

Select the Root certificate (this may be a root certificate chain) that you received from the CA you trust. The CA may be a Root Authority or an Intermediate Authority.

Click **Upload**.

The certificate is uploaded at this time, but does not persist until you click **Save**.

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)**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- 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.

2. In the **ActiveSync Configuration** section, if you are configuring Kerberos for ActiveSync:

For Server Authentication, select **Kerberos**.

Configure the ActiveSync Server SPNs:

- *If you used the fully-qualified domain name* of the ActiveSync server as the basis for the Service Principal Name of the server in the ActiveSync Server(s) field above, then *select* **Derive SPN From FQDN Of ActiveSync Server**.
- *If you configured the IP address or alternate DNS name* of the ActiveSync server in the ActiveSync Server(s) field, then *deselect* **Derive SPN From FQDN Of ActiveSync Server**.
  Enter the SPNs for each of your ActiveSync servers, separated by semicolons, in the field that appears when this option is selected. Typically, SPNs are in the form: http/<FQDN>.
  Example: `http/CAS.ironmobile.com`.

The SPN is case-sensitive. The name of the CAS node that uses KCD must exactly match the name of the node.

3. In the **App Tunneling Configuration** section, if you are configuring Kerberos for AppTunnel, for an AppTunnel Service configure the following:

For **Server Auth**, select **Kerberos**.

In the **Server SPN List** field, enter the Service Principal Name (SPN) for each server listed in the **Server List**.

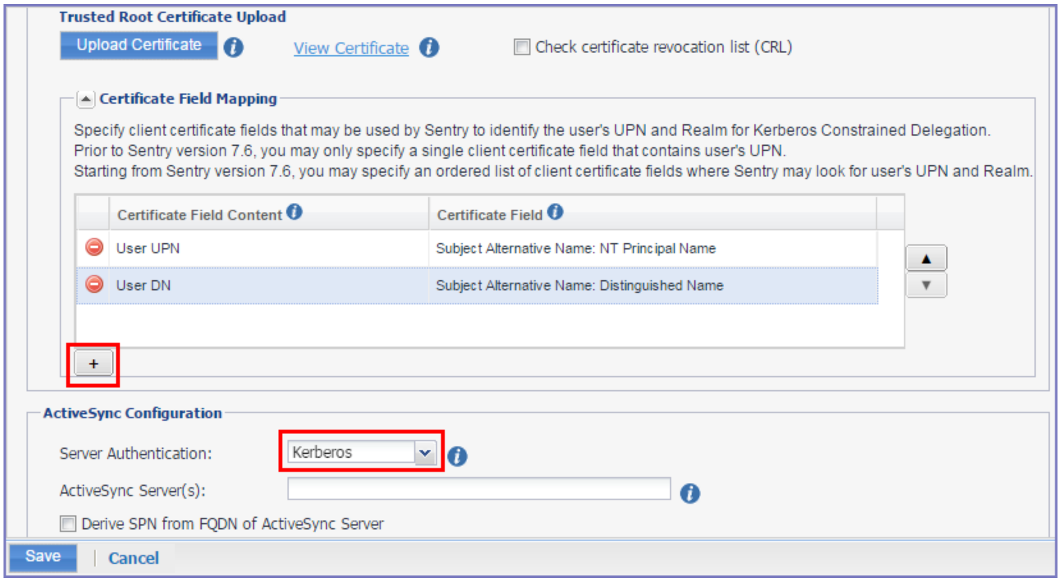
- Each SPN must be separated by semicolons.
  Example: sharepoint1.company.com;sharepoint2.company.com.
- The **Server SPN List** applies only when the Service Name is not **<ANY>** and the **Server Auth** is **Kerberos**.
- If each server in the **Server List** has the same name as its SPN, you can leave the **Server SPN List** empty. However, if you include a **Server SPN List**, the number of SPNs listed must equal the number of servers listed in the Server List. The first server in the Server List corresponds to the first SPN in the Server SPN List, the second server in the Server List corresponds to the second server in the Server SPN List, and so on.

If **Service Name** is **<ANY>** and **Server Auth** is **Kerberos**, the Standalone Sentry assumes that the SPN is the same as the server name received from the device.

4. When you select for **Identity Certificate** for **Device Authentication**, the **Certificate Field Mapping** section appears. Use this section to specify the certificate fields that Ivanti Standalone Sentry can use to derive users' UPN and Realm for Kerberos authentication. You can specify multiple certificate fields.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 5. CERTIFICATE FIELD MAPPING



Trusted Root Certificate Upload

□ Check certificate revocation list (CRL)

Certificate Field Mapping

Specify client certificate fields that may be used by Sentry to identify the user's UPN and Realm for Kerberos Constrained Delegation.
Prior to Sentry version 7.6, you may only specify a single client certificate field that contains user's UPN.
Starting from Sentry version 7.6, you may specify an ordered list of client certificate fields where Sentry may look for user's UPN and Realm.

Certificate Field Content	Certificate Field
User UPN	Subject Alternative Name: NT Principal Name
User DN	Subject Alternative Name: Distinguished Name

ActiveSync Configuration

Server Authentication: Kerberos

ActiveSync Server(s):

□ Derive SPN from FQDN of ActiveSync Server

Click **+** to add an entry.

The order of the rows specifies priority. Sentry checks the first row and if the required information is not available, it will check the next row. Use the up and down arrow keys to reorder the rows.

For **Certificate Field Content**, select **User UPN** or **User DN**.

Certificate Field Content	Certificate Field
User UPN	Select the certificate field from which Standalone Sentry will derive the user’s UPN
User DN	Select the certificate field from which Standalone Sentry will derive the user’s realm. This field is required in a cross-realm Kerberos environment.

For **Certificate Field**, select the field from which Ivanti Standalone Sentry will derive the User UPN or User DN.

For WP8.1 devices, for User UPN, select either **DNS Name** or **RFC 822 Name**, and for User DN select **Certificate Subject**.

5. Complete the **Kerberos Authentication Configuration** section.

The configuration depends on whether you use a keytab file or not.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

6. Click **Save**.

Standalone Sentry restarts.

Related topics

- For completing the Kerberos Authentication Configuration section, see "Configuring Kerberos authentication using a Kerberos-generated keytab file" below and "Configuring Kerberos authentication without a keytab file" on the next page.
- For details on configuring AppTunnel for AppConnect apps, see the AppConnect and AppTunnel Guide.
- See also, "Key Distribution Center (KDC) discovery through DNS" on page 124.
- If you are setting up tunneling to DFS servers and authenticating using Kerberos, see "Configuring Kerberos authentication for DFS" on page 127.
- For information about Kerberos setup, see the *Authentication Using Kerberos Constrained Delegation* tech note.

Configuring Kerberos authentication *using a Kerberos-generated keytab file*

Procedure

1. In the **Kerberos Authentication Configuration,** select **Use Keytab File**.
2. Click **Upload File**.
3. Select the keytab file.
4. Click **Upload**.

The keytab file provides the required Kerberos authentication information. For information about generating a keytab, see *Authentication Using Kerberos Constrained Delegation* on the Support site.

5. Optionally, configure one or more **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. Enter either the IP address or the FQDN of the AD.

You can enter multiple KDCs. Separate each KDC with a semicolon.

For example: KDCdomainname1.com;KDCdomainname2.com.

If you do not configure a KDC, the system auto-detects the KDC.

6. Click **Save**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Standalone Sentry restarts.

Configuring Kerberos authentication *without a keytab file*

Procedure

1. In the **Kerberos Authentication Configuration** section complete the Kerberos configuration fields. Use the following guidelines:
   - ***Realm***
     The Kerberos administrative domain. The realm is usually the company domain name, in all uppercase characters.
   - ***Sentry Service Principal***
     The service principal for the Sentry service account, preceded by HTTP/. For example, if the user name of the service account is sentry1_eas_kcd, the service principal would be **`HTTP/sentry1_eas_kcd`**.
   - ***Password***
     Password for the Sentry service account.
2. Optionally, configure one or more **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.

If you do not configure a KDC, the system auto-detects the KDC.

3. Click **Save**.

Standalone Sentry restarts.

Authentication using Trusted Front-End

You can configure the Ivanti 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 Ivanti Standalone 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 Ivanti Standalone Sentry.
- Additional minor changes to references to hostname in some profiles.

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Multiple trusted root certificates for device authentication

If your company uses different trusted root CA certificates for different services, you may need to upload multiple trusted root certificates to Ivanti Standalone Sentry for device authentication.

ⓘ You can only upload one certificate file for device authentication to a Ivanti Standalone Sentry. However, you can concatenate multiple root CA certificates into a single file and upload the consolidated certificate file for device authentication.

This features allows devices with client certificates issued from different certificate authorities (CAs) to authenticate with Ivanti Standalone Sentry. Uploading multiple root CA certificates reduces the need for multiple Standalone Sentrys to handle authentication for devices with identity certificates issued by different CAs.

Creating a single certificate file with multiple root CA certificates

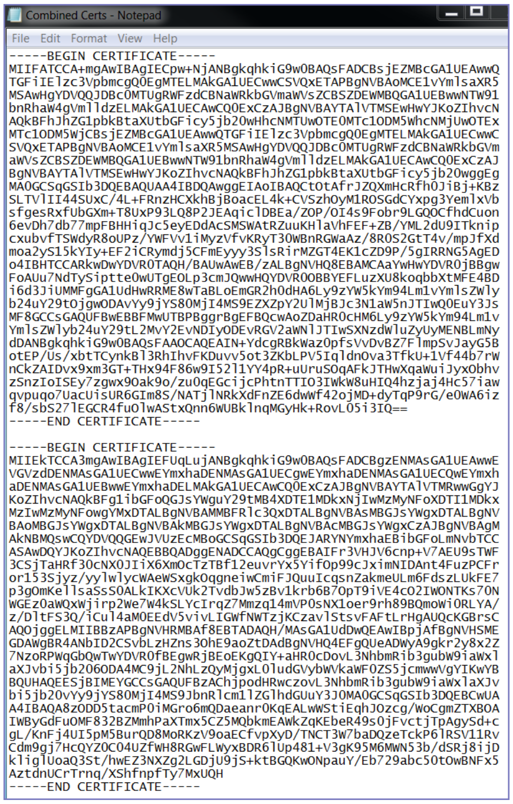
Creating a single certificate file with multiple CA certificates allows you to upload a consolidated certificate file to Ivanti Standalone Sentry for device authentication.

Procedure

1. Open a text editor, such as Notepad.
2. Copy and paste the **---Begin Certificate ---** through the **---End Certificate ---** sections of the root CA to a text file.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Figure 1. Single certificate file



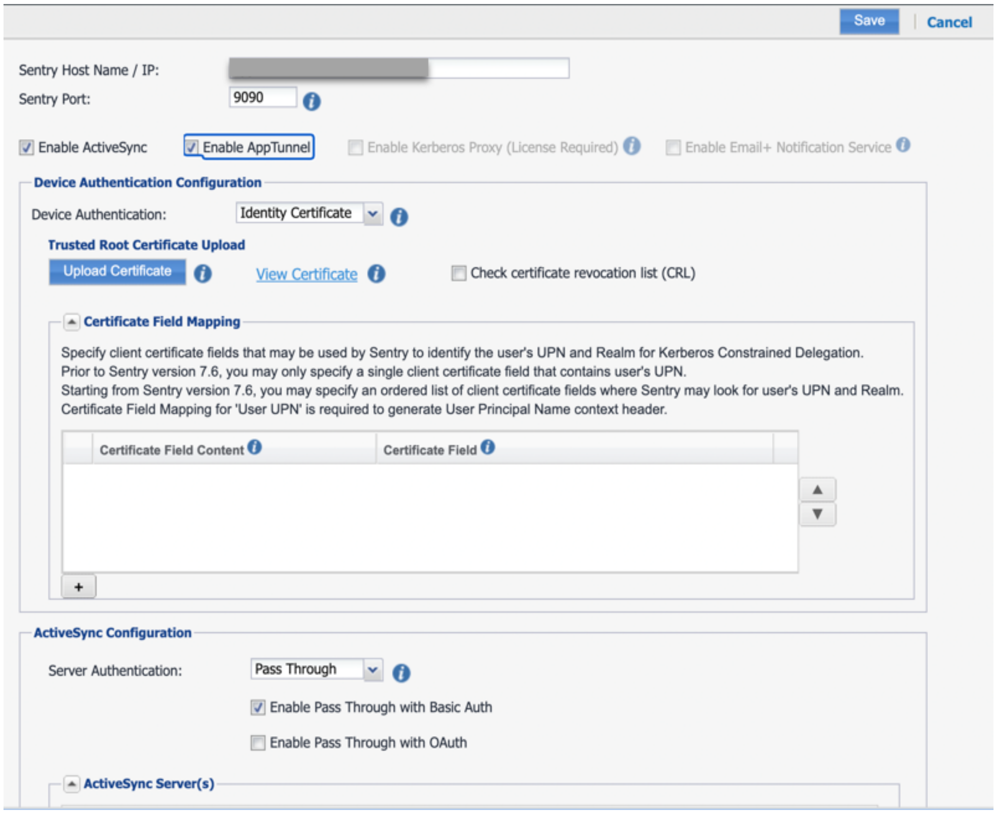
```
-----BEGIN CERTIFICATE-----
MIIFATCCA+mgAwIBAgIECpw+NjANBgkqhkiG9w0BAQsFADCBsjEZMBcGA1UEAwwQ
TGFiIElzc3VpbmcgQ0EgMTELMAkGA1UECwwCSVQxETAPBgNVBAoMCE1vYmlsaXR5
MSAwHgYDVQQJDBc0MTUgRWFzdCBNaWRkbGVmaWVsZCBSZDEWMBQGA1UEBwwNTW91
bnRhaW4gVmlldzELMAkGA1UECAwCQ0ExCzAJBgNVBAYTAlVTMSEwHwYJKoZIhvcN
AQkBFhJhZG1pbkBtaXUtbGFicy5jb20wHhcNMTUwOTE0MTc1ODM5WhcNMjUwOTEx
MTc1ODM5WjCBsjEZMBcGA1UEAwwQTGFiIElzc3VpbmcgQ0EgMTELMAkGA1UECwwC
SVQxETAPBgNVBAoMCE1vYmlsaXR5MSAwHgYDVQQJDBc0MTUgRWFzdCBNaWRkbGVm
aWVsZCBSZDEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzELMAkGA1UECAwCQ0ExCzAJ
BgNVBAYTAlVTMSEwHwYJKoZIhvcNAQkBFhJhZG1pbkBtaXUtbGFicy5jb20wggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCtOtAfrJZQXmHcRfh0JiBj+KBz
SLTVlII44SUxC/4L+FRnzHCXkhBjBoacEL4k+CVSzhOyM1ROSGdCYxpg3YemlxVb
sfgesRxfUbGXm+T8UxP93LQ8P2JEAqiclDBEa/ZOP/OI4s9Fobr9LGQOCfhdCuon
6evDh7db77mpFBHHiqJc5eyEDdAcSMSWAtRZuuKHlaVhFEF+ZB/YML2dU9ITknip
cxubvfTSWdyR8oUPz/YWFVv1iMyzVfvKRyT30WBnRGWaAz/8R0S2GtT4v/mpJfXd
moa2yS15kYIy+EF2iCRymdj5CFmEyyy3SlsRirMZGT4EK1cZD9P/5gIRRNG5AgED
o4IBHTCCARkwDwYDVR0TAQH/BAUwAwEB/zALBgNVHQ8EBAMCAaYwHwYDVR0jBBgw
FoAUu7NdTySiptte0wUTgEOLp3cmJQwwHQYDVR0OBBYEFLuzXU8koqbbXtMFE4BD
i6d3JiUMMFgGA1UdHwRRME8wTaBLoEmGR2h0dHA6Ly9zYW5kYm94Lm1vYmlsZWly
b24uY29tOjgwODAvYy9jYS80MjI4MS9EZXZpY2UlMjBJc3N1aW5nJTIwQ0EuY3Js
MF8GCCsGAQUFBwEBBFMwUTBPBggrBgEFBQcwAoZDaHR0cHM6Ly9zYW5kYm94Lm1v
YmlsZWlyb24uY29tL2MvY2EvNDIyODEvRGV2aWNlJTIwSXNzdWluZyUyMENBLmNy
dDANBgkqhkiG9w0BAQsFAAOCAQEAIN+YdcgRBkWaz0pfsVvDvBZ7FlmpSvJayG5B
otEP/Us/xbtTCynkBl3RhIhvFKDuvv5ot3ZKbLPV5IqldnOva3TfkU+1Vf44b7rW
nCkZAIDvx9xm3GT+THx94F86w9I52l1YY4pR+uUruSOqAFkJTHwXqaWuiJyxObhv
zSnzIoISEy7zgwx9Oak9o/zu0qEGcijcPhtnTTIO3IWkW8uHIQ4hzjaj4Hc57iaw
qvpuqo7UacUisUR6GIm8S/NATjlNRkXdFnZE6dwWf42ojMD+dyTqP9rG/e0WA6iz
f8/sbS27lEGCR4fuOlwAStxQnn6WUBklnqMGyHk+RovL05i3IQ==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIEkTCCA3mgAwIBAgIEFUqLujANBgkqhkiG9w0BAQsFADCBgzENMAsGA1UEAwwE
VGVzdDENMAsGA1UECwwEYmxhaDENMAsGA1UECgwEYmxhaDENMAsGA1UECQwEYmxh
aDENMAsGA1UEBwwEYmxhaDELMAkGA1UECAwCQ0ExCzAJBgNVBAYTAlVTMRwwGgYJ
KoZIhvcNAQkBFg1ibGFoQGJsYWguY29tMB4XDTE1MDkxNjIwMzMyNFoXDTI1MDkx
MzIwMzMyNFowgYMxDTALBgNVBAMMBFRlc3QxDTALBgNVBAsMBGJsYWgxDTALBgNV
BAoMBGJsYWgxDTALBgNVBAkMBGJsYWgxDTALBgNVBAcMBGJsYWgxCzAJBgNVBAgM
AkNBMQswCQYDVQQGEwJVUzEcMBoGCSqGSIb3DQEJARYNYmxhaEBibGFoLmNvbTCC
ASAwDQYJKoZIhvcNAQEBBQADggENADCCAQgCggEBAIFr3VHJV6cnp+V7AEU9sTWF
3CSjTaHRf30cNX0JIiX6XmOcTzTBf12euvrYx5YifOp99cJximNIDAnt4FuzPCFr
or153Sjyz/yylwlycWAeWSxgkOqgneiwCmiFJQuuIcqsnZakmeULm6FdszLUkFE7
p3gOmKellsaSsS0ALkIKXcVUk2TvdbJw5zBv1krb6B7OpT9iVE4cO2IWONTKs7ON
WGEz0aWQxWjirp2We7W4kSLYcIrqZ7Mmzq14mVP0sNX1oer9rh89BQmoWi0RLYA/
z/DltFS3Q/iCul4aM0EEdV5vivLIGWfNWTzjKCzavlStsvFAFtLrHgAUQcKGBrsC
AQOjggELMIIBBzAPBgNVHRMBAf8EBTADAQH/MAsGA1UdDwQEAwIBpjAfBgNVHSME
GDAWgBR4ANbID2CSvbLzHZns3OhE9aoZtDAdBgNVHQ4EFgQUeADWyA9gkr2y8x2Z
7NzoRPWqGbQwTwYDVR0fBEgwRjBEoEKgQIY+aHR0cDovL3NhbmRib3gubW9iaWxl
aXJvbi5jb206ODA4MC9jL2NhLzQyMjgxL0ludGVybWVkaWF0ZS5jcmwwVgYIKwYB
BQUHAQEESjBIMEYGCCsGAQUFBzAChjpodHRwczovL3NhbmRib3gubW9iaWxlaXJv
bi5jb20vYy9jYS80MjI4MS9JbnRlcm1lZGlhdGUuY3J0MA0GCSqGSIb3DQEBCwUA
A4IBAQA8zODD5tacmP0iMGro6mQDaeanr0KqEALwWStiEqhJOzcg/WoCgmZTXBOA
IWByGdFuOMF832BZMmhPaXTmx5CZ5MQbkmEAWkZqKEbeR49s0jFvctjTpAgySd+c
gL/KnFj4UI5pM5BurQD8MoRKzV9oaECfvpXyD/TNCT3W7baDQzeTckP6lRSV11Rv
Cdm9gj7HcQYZ0C04UZfWH8RGwFLWyxBDR6lUp481+V3gK95M6MWN53b/dSRj8ijD
kliglUoaQ3St/hwEZ3NXZg2LGDjU9jS+ktBGQKwONpauY/Eb729abc50tOwBNFx5
AztdnUCrTrnq/XShfnpfTy7MxUQH
-----END CERTIFICATE-----
```

3. Save the concatenated text file.
4. Change the extension of the text file to **.cer**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

5. Click **Upload Certificate** to upload the concatenated **.cer** file to Standalone Sentry.



Sentry Host Name / IP: [redacted]

Sentry Port: 9090

☑ Enable ActiveSync ☑ Enable AppTunnel ☐ Enable Kerberos Proxy (License Required) ☐ Enable Email+ Notification Service

Device Authentication Configuration

Device Authentication: Identity Certificate

Trusted Root Certificate Upload

☐ Check certificate revocation list (CRL)

Certificate Field Mapping

Specify client certificate fields that may be used by Sentry to identify the user's UPN and Realm for Kerberos Constrained Delegation.
Prior to Sentry version 7.6, you may only specify a single client certificate field that contains user's UPN.
Starting from Sentry version 7.6, you may specify an ordered list of client certificate fields where Sentry may look for user's UPN and Realm.
Certificate Field Mapping for 'User UPN' is required to generate User Principal Name context header.

Certificate Field Content	Certificate Field

ActiveSync Configuration

Server Authentication: Pass Through

☑ Enable Pass Through with Basic Auth

☐ Enable Pass Through with OAuth

ActiveSync Server(s)

Key Distribution Center (KDC) discovery through DNS

With Kerberos authentication, Ivanti Standalone Sentry determines which Key Distribution Center (KDC) to communicate with to obtain a ticket for a user account. If the user is located in the same realm as Standalone Sentry, the configured KDC is used. If the user is not located in the same realm, by default, Ivanti Standalone Sentry attempts to locate a KDC through DNS discovery.

KDC discovery through DNS can be triggered by one of the following:

- The user's realm is different from that of Standalone Sentry.
- Even if the user's realm is the same as Standalone Sentry, the letter case in the realms do not match exactly.
- Sometimes, the KDC that is configured cannot be resolved.

The following provide additional information about KDC discovery:

- "KDC discovery in a cross-realm Kerberos environment" on the next page.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- "Disabling Key Distribution Center (KDC) discovery through DNS" on the next page.
- "Configuring additional Kerberos realms" on the next page.

KDC discovery in a cross-realm Kerberos environment

In a cross-realm environment, discovery through DNS could be slow and even fail. This may result in failure to get a ticket. DNS discovery may be slow or fail due to the following reasons:

- The response may contain a very large list of all KDCs known to that DNS server. Going through a large set of records may take a long time.
- The topology of customer's network and access rules and firewall configuration may block or slow access to KDC servers, and Ivanti Standalone Sentry may eventually give up. Thus, failing to acquire a ticket.

To better manage the ticketing process in a cross-realm Kerberos environment, you can do the following:

- Disable KDC discovery through DNS.
- Configure additional realms, other than the Ivanti Standalone Sentry realm, and the associated KDC servers.
- If KDC discovery is disabled, you must configure additional Kerberos realms and the associated KDC servers.
- If KDC discovery is disabled, Standalone Sentry will fail to obtain a ticket in the following cases:

- the KDC server for a user’s realm is not configured in Standalone Sentry settings
- the KDC servers for that realm are not accessible

- If KDC discovery through DNS is enabled and if you have also configured additional KDC servers, Standalone Sentry will first check the configured KDC servers before doing KDC discovery through DNS.

In a cross-realm Kerberos environment, configuring Kerberos realms and the associated KDC servers:

- reduces the time required to get a ticket
- decreases the risk of failure to get a ticket

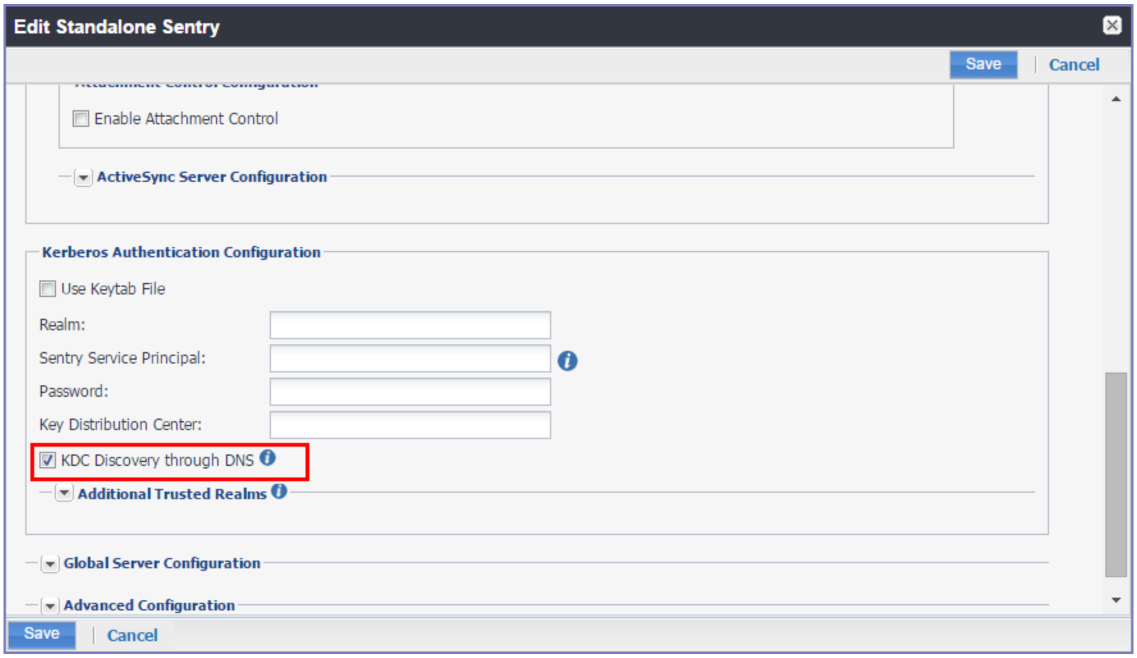
Disabling Key Distribution Center (KDC) discovery through DNS

Disabling KDC discovery through DNS allows you to better manage the ticketing process in a cross-realm Kerberos environment.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services** > **Sentry**.
2. Click on the **Edit** icon for the Sentry record that you will edit.
3. Scroll down to the **Kerberos Authentication Configuration** section.

FIGURE 1. DISABLING KDC DISCOVERY THROUGH DNS


Edit Standalone Sentry
Save
Cancel
Attachment Control Configuration
ActiveSync Server Configuration
Kerberos Authentication Configuration
Additional Trusted Realms
Global Server Configuration
Advanced Configuration
Save
Cancel

☐ Enable Attachment Control

☐ Use Keytab File

Realm:

Sentry Service Principal:

Password:

Key Distribution Center:

☑ KDC Discovery through DNS

4. De-select the **KDC Discovery through DNS** option.
5. Click **Save** to save the changes.

Related topics

"KDC discovery in a cross-realm Kerberos environment" on the previous page.

Configuring additional Kerberos realms

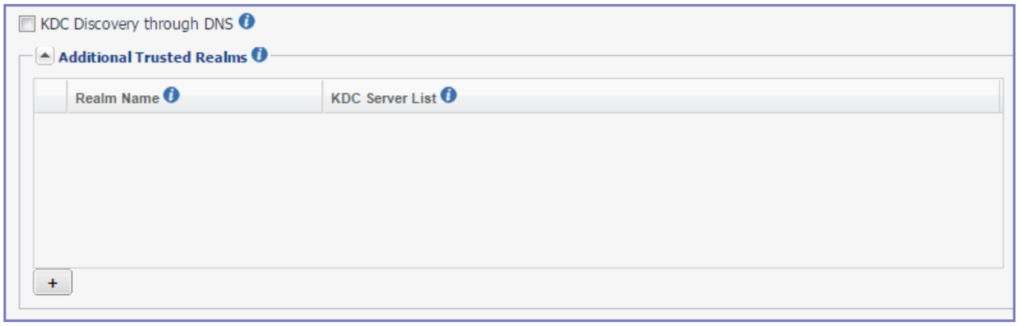
You configure additional realms, other than the Standalone Sentry realm, and the associated KDC servers to better manage the ticketing process in a cross-realm Kerberos environment.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services** > **Sentry**.
2. Click on the **Edit** icon for the Sentry record that you will edit.
3. Scroll down to the **Kerberos Authentication Configuration** section.
4. Expand the **Additional Trusted Realms** section.

FIGURE 2. ADDITIONAL TRUSTED REALMS



☐ KDC Discovery through DNS

5. Click **+** to add new Kerberos realm.

Item	Description
Realm Name	Enter a Kerberos realm name. Realm names are not case sensitive.
KDC Server List	Enter the associated KDC servers. You can enter domain name or IP address. Each domain name or IP address must be separated by a semicolon. If a port is not specified, the default port 88 is used.

6. Click **Save** to save the changes.

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 Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Before you begin

Setup Ivanti Standalone Sentry for authentication using Kerberos. See "Configuring authentication using an identity certificate and Kerberos constrained delegation" on page 116.

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:

Sign in to the Ivanti Standalone Sentry system manager.

Go to **Settings > Static Hosts**.

Click **Add**.

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

Click **Save.**

Related topics

- "Static Hosts" on page 182.

Cross-realm Kerberos support

Support for cross-realm Kerberos on the Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

ActiveSync Policies

The following describe the ActiveSync policy use with Ivanti Standalone Sentry:

About the ActiveSync policy

Ivanti Standalone Sentry pushes an ActiveSync policy to a device if you have applied an ActiveSync policy to that device. If an ActiveSync policy is not applied to the device, the device interaction with the ActiveSync server is determined by the settings in the **Default ActiveSync Policy behavior** configured in the Sentry **Preferences** page.

Integrated Sentry provides the ActiveSync policies to the Microsoft Exchange Server, which pushes the appropriate policy to each ActiveSync device.

Use the ActiveSync policy settings to configure the following:

- Password requirements for end-user access to the device
- Features to disable, such as text messaging or desktop syncing
- Device encryption requirements
- The maximum number of devices that can have the same mailbox

  This setting is used by Ivanti EPMM and Sentry, but is not pushed to the device.

The default ActiveSync policy is not applicable when you use Integrated Sentry.

The device applies the policy's settings as far as its capabilities allow; not all devices support all the settings in an ActiveSync policy.

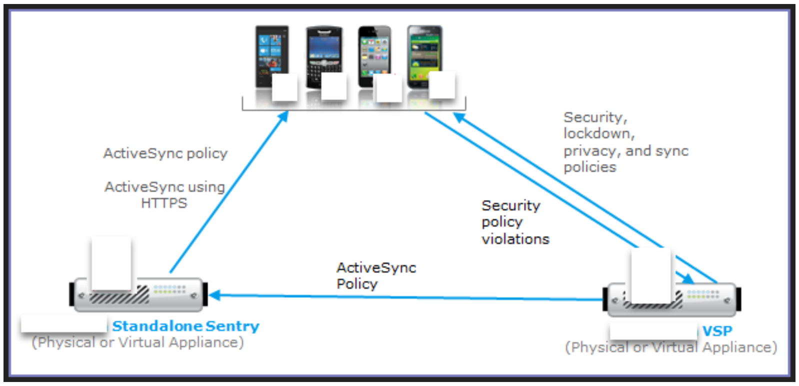
If a device *is* registered, then Ivanti EPMM applies security, lockdown, privacy, and sync policies to the device. These policies are applied to the device directly from Ivanti EPMM, based on label assignments. Because these policies provide detailed management for *registered* ActiveSync devices, ActiveSync policies are only useful in the following cases:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- An ActiveSync device is unregistered.
- An ActiveSync device cannot support the Ivanti EPMM-provided policies.

The following illustration shows how Ivanti Standalone Sentry pushes the ActiveSync policy to the device, but Ivanti EPMM applies the other policies to the device. It also shows that Ivanti EPMM finds out that a device is in violation of its security policy, but does not know if the device is in violation of its ActiveSync policy.

FIGURE 1. ACTIVESYNC POLICY AND IVANTI EPMM INTERACTION


ActiveSync policy
ActiveSync using HTTPS
Security, lockdown, privacy, and sync policies
Security policy violations
ActiveSync Policy
Standalone Sentry
(Physical or Virtual Appliance)
VSP
(Physical or Virtual Appliance)

The following sections provide additional information:

- "Default ActiveSync Policy behavior" below
  - "The ActiveSync mailbox policy on the ActiveSync server" on the next page
  - "ActiveSync server refresh policy interval" on the next page
  - "The security policy versus the ActiveSync policy" on page 132

Default ActiveSync Policy behavior

If an ActiveSync policy is not applied, the device interaction with the ActiveSync server is determined by the settings in the **Default ActiveSync Policy behavior**.

The **Default ActiveSync Policy behavior** determines whether Sentry applies the ActiveSync server’s policy to the device syncing with the ActiveSync server.

The default ActiveSync policy behavior for the Standalone Sentry is configured in the **Services > Sentry > Preferences** page in the Admin Portal. The **Default ActiveSync Policy behavior** is applied if an ActiveSync policy is not applied to the device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

See also, "Changing the default ActiveSync policy behavior" on page 147.

The ActiveSync mailbox policy on the ActiveSync server

An ActiveSync server can also have ActiveSync policies, sometimes called *ActiveSync mailbox policies*. The ActiveSync server can push an ActiveSync mailbox policy to the device in the following cases:

- You are not using Sentry.

- You are using a Ivanti Standalone Sentry with the following settings:

- A ActiveSync policy is not applied to the device.
- The Default ActiveSync Policy behavior is set to **Apply AS Server policy**.

- You are using Integrated Sentry. Integrated Sentry provides the ActiveSync policies to the Microsoft Exchange Server, which updates its set of ActiveSync mailbox policies, and pushes the appropriate policy to each ActiveSync device.

The ActiveSync server does the following when a device attempts to access its email:

- Compares the device’s settings with the server’s appropriate ActiveSync mailbox policy.

- Rejects the device’s access attempt if the device’s settings do not comply with the policy.

- The settings available in the ActiveSync policy are a subset of the settings available in the ActiveSync mailbox policy on the ActiveSync server.

  - The values of settings in the ActiveSync policy can be different than the values in the ActiveSync mailbox policy on the ActiveSync server.

  - When using Ivanti Standalone Sentry, if the ActiveSync mailbox policy on the ActiveSync server is more restrictive than the ActiveSync policy, the ActiveSync server rejects the device’s attempts to access the ActiveSync server. Therefore, a best practice is to make the ActiveSync policy equal to or more restrictive than the ActiveSync server’s policy.

ActiveSync server refresh policy interval

The ActiveSync policy and the ActiveSync server’s ActiveSync mailbox policy both have a setting called “refresh policy interval”. This setting tells how often the ActiveSync server refreshes the ActiveSync policy on the device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

When using Ivanti Standalone Sentry, set the refresh policy interval on the ActiveSync server’s ActiveSync mailbox policies as follows:

- If all the devices access the ActiveSync server through Ivanti Standalone Sentry, disable the refresh policy interval for the ActiveSync mailbox policies on the ActiveSync server. It is not applicable because Standalone Sentry manages which ActiveSync policies are pushed to the devices and when. Setting the interval in the ActiveSync mailbox policy on the ActiveSync server can introduce delays in email synchronization.

- If *some* devices access the ActiveSync Server directly, without going through Standalone Sentry, set the refresh policy interval for the ActiveSync mailbox policies on the ActiveSync server to several hours.

If you are using Integrated Sentry, set the refresh policy interval of the ActiveSync policies to several hours. Integrated Sentry passes the ActiveSync policies to the Microsoft Exchange Server, which updates its ActiveSync mailbox policies.

The security policy versus the ActiveSync policy

The security policy has many settings. It has the following settings in common with the ActiveSync policy:

- Password requirements

- Device encryption requirements

However, the security policy and ActiveSync policy are used differently.

Ivanti Standalone Sentry (or the Microsoft Exchange Server when using Integrated Sentry) pushes an ActiveSync policy to the device using the ActiveSync protocol. The device applies the following settings from the policy, as far as the device’s capabilities allow:

- Password requirements

- Device encryption

- Lockdown settings

Ivanti EPMM is not aware of whether these ActiveSync policy settings are successfully applied on a device. Ivanti EPMM is aware only of the ActiveSync policy setting that limits the number of devices with the same mailbox. If that limit is exceeded, Ivanti EPMM tells Sentry to block the additional device from accessing the mail server.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

However, Ivanti EPMM *is* aware if a device violates the security policy. Ivanti EPMM detects a security policy violation on the device when, for example, the device checks in with Ivanti EPMM. You can configure the security policy so that upon detection of the security policy violation, Ivanti EPMM tells Sentry to block the device's access to the ActiveSync server. You can also configure the security policy to alert an administrator and the user of the violation.

Some types of registered devices, such as WebOS devices, do not support the security policy. Therefore, such devices, although registered, use *only* the ActiveSync policy. On these devices, you depend on the ActiveSync policy to appropriately secure the device.

Most devices do support the security policy, and therefore, most devices that are registered *and* access the ActiveSync server use both policies. However, consider the case where the ActiveSync policy and the security policy have different password requirements. Depending on the device type, this case can lead to unexpected behavior. **As a best practice, configure the ActiveSync policy and security policy to have the same settings for password requirements and device encryption.**

See the following for additional information:

- "Device usage of the ActiveSync and security policies" below.
  - "Policy application on commonly used device platforms" on the next page.
  - "Comparison of ActiveSync policy and security policy settings" on the next page.
  - "System behavior regarding ActiveSync and security policies" on page 135.

Device usage of the ActiveSync and security policies

An ActiveSync device can be either registered or unregistered. Furthermore, a registered device is not necessarily an ActiveSync device. For example, when using Ivanti Standalone Sentry, if a registered device has not yet accessed the ActiveSync server, Ivanti EPMM does not consider it an ActiveSync device.

The following table summarizes how devices in any of these combinations use the ActiveSync and security policies.

TABLE 21. ACTIVESYNC POLICY AND SECURITY POLICY USE

ActiveSync device	Registered	Unregistered
Yes	ActiveSync policy Security policy, if the device type supports security policies	ActiveSync policy
No	Security policy, if the device type supports security policies	

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

ⓘ The ability of a specific device to apply the policies' settings can vary.

Policy application on commonly used device platforms

The following table shows how some commonly used device platforms and email clients apply the security policy and ActiveSync policy:

TABLE 22. ACTIVESYNC POLICY AND SECURITY POLICY APPLICATION

Device platform / email client	Behavior regarding applying the ActiveSync and security policies
iOS Mail client	Applies the strictest policy.
Android with NitroDesk's Touchdown email client	Applies only the security policy.
Android on Samsung devices with Samsung native email client	Applies strictest password policy. Encryption policies must be the same.

Comparison of ActiveSync policy and security policy settings

The following table summarizes the differences between the settings of ActiveSync and security policies:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 23. DIFFERENCES IN SETTINGS FOR ACTIVESYNC AND SECURITY POLICIES

	ActiveSync policy	**Security policy**
Specifies password requirements for accessing the device	Yes	Yes
Specifies device encryption requirements	Require device encryption: Block ActiveSync server access if the device does not support and enable device encryption. Enable device encryption: Enable device encryption if available.	Whether device encryption is required, and for what data types. Whether to encrypt the SD card.
Specifies maximum devices that can have the same mailbox	Yes	No
Specifies access control policies, such as device OS version requirements, application requirements, and more.	No	Yes
Specifies the maximum time a device can be out of contact before it is wiped.	No	Yes

System behavior regarding ActiveSync and security policies

The following table summarizes the differences between the behavior of your deployment with regard to ActiveSync and security policies:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 24. ACTIVESYNC AND SECURITY POLICY BEHAVIOR

	ActiveSync policy	**Security policy**
Standalone Sentry pushes the policy to the device.	Yes	No
Integrated Sentry provides the policy to the Microsoft Exchange Server, which pushes it to the device.	Yes	No
Ivanti EPMM detects policy violations.	No	Yes
Specifies whether to block ActiveSync server access when a policy violation occurs.	No	Yes
The policy applies to devices with a specified mailbox.	Yes	No
The policy applies to devices according to label assignments.	No	Yes

ActiveSync policy settings

ActiveSync policies specify settings to apply to selected ActiveSync devices. ActiveSync devices use the ActiveSync protocol to connect to an ActiveSync server to access a user’s email, calendar, tasks, contacts.

Ivanti recommends assigning a ActiveSync policy to devices other than iOS, Android, and WP8 devices.

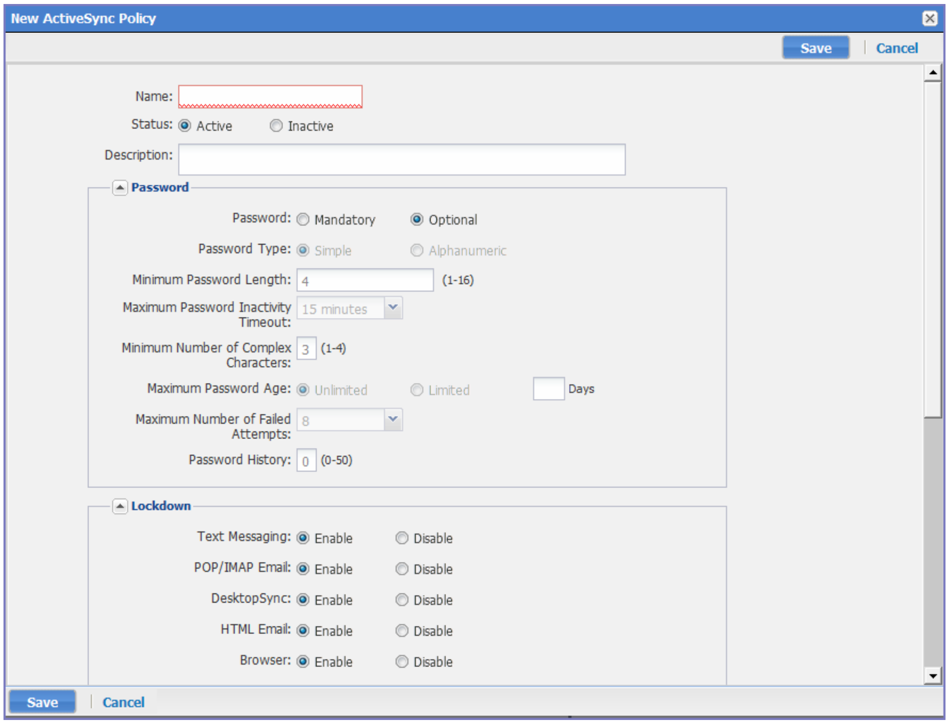
Also, see the following information:

- “Working with security policies,” in the *Ivanti EPMM Device Management Guide* for detailed information about security policies.
- “Working with policies,” in the Ivanti EPMM Device Management Guide for information on general procedures for creating, editing, and applying policies.

To work with ActiveSync policies, from the Admin Portal go to **Policies & Configs > ActiveSync Policies**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Figure 1. ActiveSync policy settings



Name:

Status: ● Active ○ Inactive

Description:

Password

Password: ○ Mandatory ● Optional

Password Type: ● Simple ○ Alphanumeric

Minimum Password Length: 4 (1-16)

Maximum Password Inactivity Timeout: 15 minutes

Minimum Number of Complex Characters: 3 (1-4)

Maximum Password Age: ● Unlimited ○ Limited Days

Maximum Number of Failed Attempts: 8

Password History: 0 (0-50)

Lockdown

Text Messaging: ● Enable ○ Disable

POP/IMAP Email: ● Enable ○ Disable

DesktopSync: ● Enable ○ Disable

HTML Email: ● Enable ○ Disable

Browser: ● Enable ○ Disable

The following table describes the settings for configuring an ActiveSync policy:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 25. ACTIVESYNC POLICY SETTINGS DESCRIPTION

Item	Description	Default Policy Setting
Name	Required. Enter a descriptive name for this policy. This is the text that will be displayed to identify this policy throughout the Admin Portal. This name must be unique within this policy type. Though using the same name for different policy types is allowed (e.g., Executive), consider keeping the names unique to ensure clearer log entries.	Default ActiveSync Policy
Status	Select Active to turn on this policy. Select Inactive to turn off this policy.	Active
Description	Enter an explanation of the purpose of this policy.	
Password		
Password	Select Mandatory to specify that the user must enter a password before being able to access the device. Otherwise, select Optional, which allows the user to determine whether the password will be set. ⓘ If you intend to use the Lock feature in case the phone is lost or stolen, then a password must be set on the phone. Therefore, specifying a mandatory password is strongly advised.	Optional
Password Type	Specify whether the password should be simple numeric input, be restricted to alphanumeric characters, or have no restrictions (that is, Don’t Care).	Simple
Minimum Password Length	Enter a number between 1 and 10 to specify the minimum length for the password. Leave this setting blank to specify no minimum.	
Maximum Password Inactivity Timeout	Select the maximum amount of time to allow as an inactivity timeout. The user can then specify up to this value as the interval after which the password must be re-entered.	
Minimum Number of Complex Characters	Specify the minimum number of special characters that must be included in a password.	

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 25. ACTIVESYNC POLICY SETTINGS DESCRIPTION (CONT.)

Item	Description	Default Policy Setting
Maximum Password Age	Select Unlimited or Limited to indicate whether to enforce limits on password age. If you select Limited, specify the numbers of days after which the password will expire.	
Maximum Number of Failed Attempts	Specify the maximum number of times the user can enter an incorrect password before all access is denied. Select a number between 4 and 16.	
Password History	Specify the number of passwords remembered to ensure that users define a different password. For example, if you want to prevent users from repeating a password for the next four password changes, enter 4.	
Lockdown		
Text Messaging	Specify whether to enable text messaging on the phone via ActiveSync.	Enable
POP/IMAP Email	Specify whether to enable email forwarding access on the phone via ActiveSync.	Enable
DesktopSync	Specify whether to enable DesktopSync on the phone.	Enable
HTML Email	Specify whether to enable HTML Email access on the phone.	Enable
Browser	Specify whether to enable browser access on the phone.	Enable
Security		
Policy Refresh Interval	Specify the time that should elapse between attempts to synchronize policy settings with the ActiveSync server.	Limited: 0 Days, 0 Hours
Block ActiveSync connection for smartphone when	Select “Per-Mailbox smartphone count exceeds” to block ActiveSync connections if too many devices have the same mailbox. Specify the number of devices to set as the limit. When the limit is exceeded, the last device that attempts to access the ActiveSync server is blocked.	
Data Encryption		
Require Device Encryption	Specifies whether the device should be blocked from accessing the ActiveSync server if the device does not support encryption.	Off

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 25. ACTIVESYNC POLICY SETTINGS DESCRIPTION (CONT.)

Item	Description	Default Policy Setting
Enable Device Encryption	Specifies whether to automatically turn on encryption if the phone supports it.	Off
Search Mailboxes	Enter a portion of the mailbox ID to find a mailbox. ℹ This field is not available for the default ActiveSync policy for Standalone Sentry.	None
Apply to Mailboxes	Apply the policy to the selected mailboxes. Starting with Ivanti Standalone Sentry version 4.5, mailboxes configured in an ActiveSync policy only enforce the number of devices set in the Per-Mailbox smartphone count exceeds field. To manage devices with the ActiveSync policy, you must manually apply the ActiveSync policy to each device. In earlier versions of Sentry, the ActiveSync policy is automatically applied to devices with mailboxes configured in the policy. The Default ActiveSync Policy is automatically applied to devices that do not have mailboxes configured in an ActiveSync policy. ℹ This field is not available for the default ActiveSync policy for Standalone Sentry.	Default not applicable

View number of ActiveSync devices

In the **ActiveSync Policies** page, the **# Phones** for an ActiveSync Policy displays the number of devices to which the policy is applied. Since assigning an ActiveSync policy to iOS, Android, and WP8 devices is not recommended, you may only see devices other than iOS, Android, WP8.

Assign an ActiveSync policy

The ActiveSync policy is assigned to a device in the **Devices &Users > ActiveSync** page.

See also, "Assign policy" on page 161.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Managing Sentry

The following provide information about taking action on a Sentry entry, viewing Sentry information, setting Sentry preferences, and managing the Sentry certificate:

Editing, deleting, disabling, and enabling a Sentry entry in Ivanti EPMM

This sections describes how to edit, delete, disable, and enable a Sentry entry in the Admin Portal.

- "Editing a Sentry entry" below
- "Deleting a Sentry entry" on the next page
- "Disabling a Sentry entry" on the next page
- "Enabling a Sentry entry" on the next page

Editing a Sentry entry

Select the Sentry entry in the Ivanti EPMM Admin Portal to edit the Sentry settings.

Procedure

1. In the Ivanti EPMM Admin Portal, select **Services** > **Sentry**.
2. Select the entry to be edited.
3. Click the **Edit** icon next to the entry.
4. Make the necessary changes.
5. Click **Save**.

To verify that the changes are pushed to Sentry, check that the **Status** shows **Success**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Deleting a Sentry entry

Do not remove a Ivanti Standalone Sentry entry without first making sure that no devices are using Exchange app settings that use that Ivanti Standalone Sentry. Devices with such Exchange app settings are still accessing the Ivanti Standalone Sentry. These devices can continue to access the ActiveSync server even if they violate their security policy or if you manually attempt to block them. See “Exchange settings” in the Ivanti EPMM Device Management Guide.

Procedure

1. In the Ivanti EPMM Admin Portal, select **Services > Sentry**.
2. Select the entry to be deleted.
3. Click **Delete**.
4. Click **Yes** to the verification prompt.

Disabling a Sentry entry

If a Sentry is not reachable, processes like retiring a device, pin registration, or deleting a record from the Devices page may be blocked. A Sentry may be unreachable when you are performing maintenance tasks or the connection is down. The Enable and Disable options allow you to actively enable or disable any updates or notification from Ivanti EPMM to Sentry.

When you disable Sentry, the notifications from Ivanti EPMM to Sentry are disabled. This allows Ivanti EPMM processes to continue without any disruption, and it keeps the Sentry configuration. The disabled Sentry continues to process traffic from clients and continues to communicate with Ivanti EPMM.

Procedure

1. In the Admin portal, go to **Services > Sentry**.
2. Select the Sentry.
3. Click **Disable**.

The Disable option is only available if the Sentry is enabled.

4. In the pop-up dialog, click **Yes**.

The State for the Sentry in **Services > Sentry** will show **Disabled**.

The message for the Sentry in **Settings > Service Diagnostics** will show that the Sentry has been disabled.

You can change the Sentry setting when it is disabled.

Enabling a Sentry entry

When you re-enable Sentry, notifications from Ivanti EPMM to Sentry are re-established.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Admin portal, go to **Services** > **Sentry**.
2. Select the Sentry.
3. Click **Enable**.

The Enable option is only available if the Sentry is disabled.

4. In the pop-up dialog, click **Yes**.

The State for the Sentry in **Services** > **Sentry** will show **Enabled**.

The message for the Sentry in **Settings** > **Service Diagnostics** will show that the Sentry is reachable.

Any changes made to the Sentry settings will be pushed to the Sentry.

When you disable or enable a Sentry, the warning message indicates that Sentry is restarted. Only Standalone Sentry is restarted. Integrated Sentry is not restarted when it is disabled or enabled.

Viewing Sentry information

Select the Sentry entry in the Ivanti EPMM Admin Portal to view the Sentry settings.

Procedure

1. In the Ivanti EPMM Admin Portal, go to **Services** > **Sentry**.

The Sentry page lists all the Sentry servers configured on that Ivanti EPMM.

2. Select a Sentry to view additional information for that Sentry.

Additional information about the Sentry is displayed in the **Sentry Details** pane on the right.

Related topics

"Information displayed for each Sentry entry" below

Information displayed for each Sentry entry

The following information is displayed in the Sentry page for each Sentry:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 26. INFORMATION DISPLAYED FOR EACH SENTRY ENTRY

Item	Description
Type	The Sentry type. This can be either Integrated Sentry or Standalone.
Server	The Sentry hostname. Click on the link to go to the Standalone Sentry System Manager.
Port	The port that Ivanti EPMM uses to access Sentry.
View Certificate	Allows you to view the Sentry certificate. Click on the link to the view the current Sentry certificate.
Manage Certificate	Allows you to upload or generate a Sentry certificate. See "Sentry preferences" below.
State	Enabled: Ivanti EPMM can communicate with Sentry Disabled: Ivanti EPMM cannot communicate with Sentry. See "Disabling a Sentry entry" on page 142.
Status	Indicates if Ivanti EPMM is successful in communicating with Sentry.
Error	Indicates if there is an error in communicating with Sentry.

Sentry preferences

Using **Services** > **Sentry** > **Preferences** in the Admin Portal, you can set the following preferences for the integration with ActiveSync:

- Auto Block Unregistered (unlinked) Devices

See "Auto blocking unregistered devices" on the next page.

- Strict ActiveSync to device linking

See "Configuring strict ActiveSync to device linking" on page 146

- Integrated Sentry Sync Interval

See "Setting the Integrated Sentry Sync Interval" on page 146.

- Service Account Notification Email

See "Setting the Service Account Notification Email" on page 146

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Default ActiveSync behavior

See "Changing the default ActiveSync policy behavior" on page 147

- Regenerate attachment key

See "Regenerating the encryption key" on page 59

Auto blocking unregistered devices

By default, Sentry allows unregistered devices to access the ActiveSync server. Use this setting to change Sentry’s behavior to block unregistered devices from access.

When you select Yes for Auto Block Unregistered(unlinked) Devices, Sentry will not block existing unregistered devices. The sync status in the ActiveSync page will continue to display as Allowed for unregistered devices. Ivanti EPMM does not re-evaluate the sync status for existing unregistered devices. To block access to existing unregistered devices, Remove the devices from the ActiveSync page. When the device tries to access the ActiveSync server the new rule will be applied.

Blocking unregistered devices automatically blocks Windows 7 and other devices that cannot register with Ivanti EPMM. Windows 7, Windows 8 Pro, and Windows 8 RT devices cannot register with Ivanti EPMM because these devices do not have device management features. To allow these devices to sync with the ActiveSync server, Auto Block Unregistered Devices must be set to No.

When you change this setting, Ivanti Standalone Sentry immediately changes its behavior to reflect the setting. Integrated Sentry informs the Microsoft Exchange Server to change its behavior the next time Integrated Sentry syncs with Ivanti EPMM.

Procedure

1. In the Admin Portal, go to **Services** > **Sentry** > **Preferences**.
2. Select **Yes** for **Auto Block Unregistered Devices**.
3. Click **Save** to save the changes.

Related topics

For other methods for blocking devices from accessing the ActiveSync server, see the following:

- "Block" on page 160.
- “Working with security policies” in the *Ivanti EPMM Device Management Guide*.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configuring strict ActiveSync to device linking

In case Ivanti Standalone Sentry cannot successfully link an ActiveSync record to a managed device record using the ActiveSync ID, it makes additional attempts using username and email information. This may, in some cases, result in an incorrect association. Enable **Use Strict ActiveSync to Device Linking** to avoid incorrect association between an ActiveSync record and a Device record.

The default setting for **Use Strict ActiveSync to Device Linking** is **No**. This means that Standalone Sentry will make additional attempts to associate the ActiveSync record to a managed device.

Procedure

1. In the Admin Portal, go to **Services** > **Sentry** > **Preferences**.
2. For **Use Strict ActiveSync to Device Linking**, select **Yes**.
3. Click **Save**.

With strict linking, some ActiveSync records may not be automatically linked to a managed device. In these cases, you can use the **Link To** action in the ActiveSync page to manually associate the ActiveSync record to the managed device record.

Setting the Integrated Sentry Sync Interval

The Sentry Sync Interval is only applicable to Integrated Sentry. This setting tells how often Integrated Sentry performs a periodic differential sync.

Procedure

1. In the Admin Portal, go to **Services** > **Sentry** > **Preferences**.
2. Set the **Sentry Sync Interval** to the preferred interval.

Setting the Service Account Notification Email

Configure this setting if you use a Standalone Sentry that uses Kerberos for device authentication. This setting specifies the email addresses to notify if the Kerberos service account is locked, disabled, or about to expire.

Procedure

1. In the Admin Portal, go to **Services** > **Sentry** > **Preferences**.
2. In the **Service Account Notification Email** field, enter one or more email addresses. Separate the email addresses with commas.

Related topics

For more information, see *Authentication Using Kerberos Constrained Delegation*.

Changing the default ActiveSync policy behavior

The Default Active Sync policy is applied if an ActiveSync policy is not applied to the device.

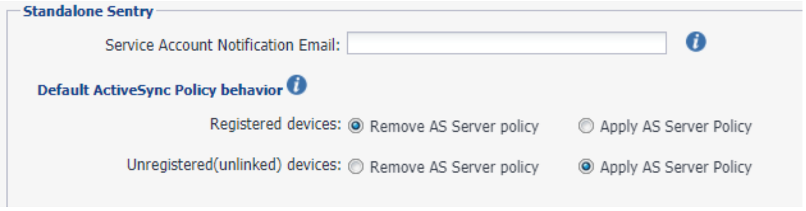
The **Default ActiveSync Policy behavior** setting determines whether Sentry applies the ActiveSync server's policy to the device syncing with the ActiveSync server.

- It may take up to twenty-four hours for any changes to the **Default ActiveSync Policy behavior** to take effect.
- As best practice, Ivanti recommends disabling the Refresh Interval on the client access server's (CAS) ActiveSync policy

Procedure

1. In the Admin Portal, go to **Services > Sentry > Preferences**.

Figure 1. Default ActiveSync policy behavior



Standalone Sentry

Service Account Notification Email:

Default ActiveSync Policy behavior

Registered devices: ● Remove AS Server policy ○ Apply AS Server Policy

Unregistered(unlinked) devices: ○ Remove AS Server policy ● Apply AS Server Policy

2. For **Default ActiveSync Policy behavior**, set the default behavior.

Item	Description
Remove AS Server policy	The ActiveSync server's policy is not applied to the device.
Apply AS Server policy	The ActiveSync server's policy is applied to the device.

3. Click **Save**.

Regenerating the attachment key

See "Regenerating the encryption key" on page 59.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry certificate

When you first install Ivanti Standalone Sentry, a self-signed certificate is also installed. Ivanti strongly recommends that you replace the default certificate with a publicly trusted certificate. Standalone Sentry presents this certificate to devices so that the devices know that the Sentry server is a trusted server. Sentry also presents its certificate to other servers connecting to it, such as a server that performs health checks on Sentry.

This certificate is not the same as:

- The certificate that devices use to authenticate themselves to Sentry.

  For information about device certificates, see "Device and Server Authentication" on page 109.

- The portal certificate that Sentry presents to browsers to identify itself as a trusted server.

  For more information, see "Certificate Management" on page 232.

The Ivanti Standalone Sentry certificate can be one of the following:

- A certificate from a trusted Certificate Authority (CA), such as Verisign or Entrust.

- A self-signed certificate.

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

You can upload and view the Ivanti Standalone Sentry certificate from the **Services > Sentry** page on the Admin Portal.

To get a certificate from a trusted Certificate Authority (CA), use the Sentry page on the Admin Portal 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 Ivanti EPMM, which sends it to Sentry.

Generating a CSR for Sentry

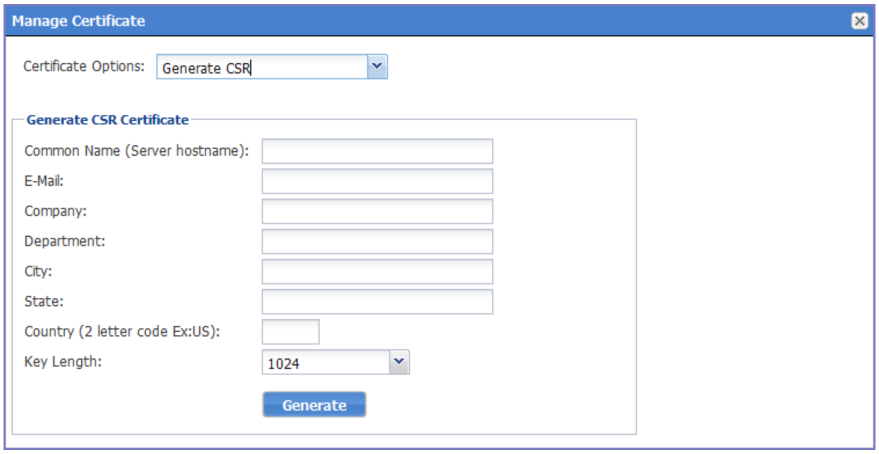
You can use the Admin Portal to generate a certificate signing request (CSR) to a Certificate Authority (CA).

Procedure

1. In the Admin Portal, go to **Services > Sentry**.
2. Click the **Manage Certificate** link.
3. For **Certificate Options**, select **Generate CSR**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Figure 1. Generate CSR



Manage Certificate

Certificate Options: Generate CSR

Generate CSR Certificate

Common Name (Server hostname):

E-Mail:

Company:

Department:

City:

State:

Country (2 letter code Ex:US):

Key Length: 1024

4. Use the following guidelines to complete the form:

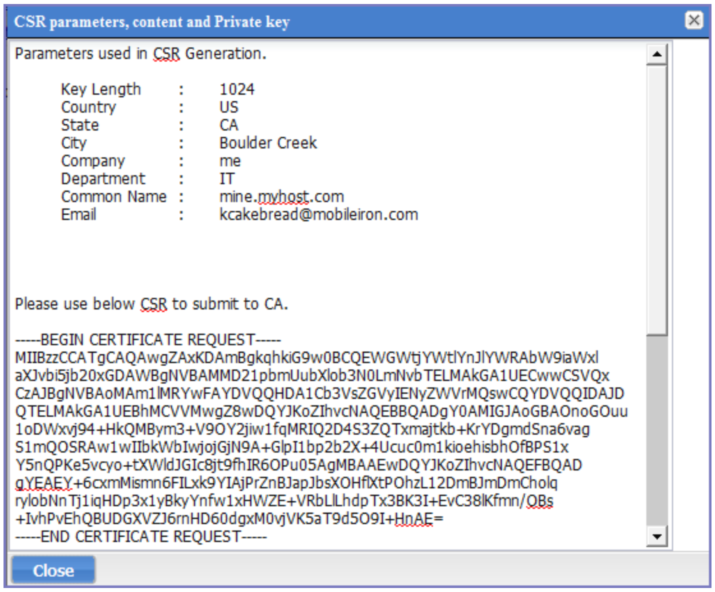
Field	Description
Common Name	Enter the server host name.
E-Mail	Enter the email address of the contact person in your organization who should receive the resulting certificate.
Company	Enter the name of the company requesting the certificate.
Department	Enter the department requesting the certificate.
City	Enter the city in which the company is located.
State	Enter the state in which the company is located.
Country	Enter the two-character abbreviation for the country in which the company is located.
Key Length	Select 1024 or 2048 to specify the length of each key in the pair.

5. Click **Generate**.

A message similar to the following displays.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 2. CSR PARAMETERS



```
Parameters used in CSR Generation.

        Key Length    :    1024
        Country       :    US
        State         :    CA
        City          :    Boulder Creek
        Company       :    me
        Department    :    IT
        Common Name   :    mine.myhost.com
        Email         :    kcakebread@mobileiron.com


Please use below CSR to submit to CA.

-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgZAxKDAmBgkqhkiG9w0BCQEWGWtjYWtlYnJlYWRAbW9iaWxl
aXJvbi5jb20xGDAWBgNVBAMMD21pbmUubXlob3N0LmNvbTELMAkGA1UECwwCSVQx
CzAJBgNVBAoMAm1lMRYwFAYDVQQHDA1Cb3VsZGVyIENyZWVrMQswCQYDVQQIDAJD
QTELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOnoGOuu
1oDWxvj94+HkQMBym3+V9OY2jiw1fqMRIQ2D4S3ZQTxmajtkb+KrYDgmdSna6vag
S1mQOSRAw1wIIbkWbIwjojGjN9A+GlpI1bp2b2X+4Ucuc0m1kioehisbhOfBPS1x
Y5nQPKe5vcyo+tXWldJGIc8jt9fhIR6OPu05AgMBAAEwDQYJKoZIhvcNAQEFBQAD
gYEAEY+6cxmMismn6FILxk9YIAjPrZnBJapJbsXOHflXtPOhzL12DmBJmDmCholq
rylobNnTj1iqHDp3x1yBkyYnfw1xHWZE+VRbLlLhdpTx3BK3I+EvC38lKfmn/QBs
+IvhPvEhQBUDGXVZJ6rnHD60dgxM0vjVK5aT9d5O9I+HnAE=
-----END CERTIFICATE REQUEST-----
```

6. Copy the content between BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST to a text file.
7. Copy the content between BEGIN RSA PRIVATE KEY and END RSA PRIVATE KEY to another text file.
8. Click **OK**.
9. Submit the file you created in step "Copy the content between BEGIN CERTIFICATE REQUEST and END CERTIFICATE REQUEST to a text file." above to the certifying authority.

Uploading Sentry certificates

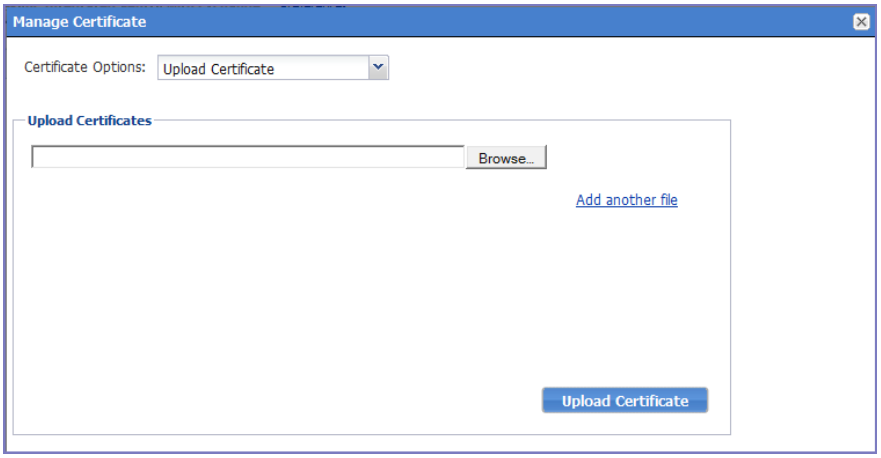
You upload the Sentry certificate in the Ivanti EPMM Admin Portal.

Procedure

1. In the Admin Portal, go to select **Services** > **Sentry**.
2. Click the **Manage Certificate** link.
3. For **Certificate Options**, select **Upload Certificate**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 3. UPLOAD CERTIFICATE



4. Click **Browse** and select a file to be uploaded. If there are additional files, click **Add another file**.

Select the certificates as indicated in the following table:

Certificate	File to Select
Key file	The file created in "Generating a CSR for Sentry" on page 148.
Server certificate	The CA certificate file you received from the certifying authority.
CA certificate	The generic CA certificate file.

5. Click **Upload Certificate**.

Viewing a Sentry certificate

You can view the contents of the Sentry certificate in the Ivanti EPMM Admin Portal.

Procedure

1. Select **Services > Sentry** in the Admin Portal.
2. Click **View Certificate**.

Changing the Standalone Sentry certificate

Changing the Sentry certificate will impact email, AppTunnel, and Ivanti Tunnel deployments. The AppTunnel AppConfig and Ivanti Tunnel VPN configurations will have to be re-pushed to devices. If you are uploading a new self-signed certificate, the new certificate will have to be re-pushed to devices.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. Upload the Sentry certificate in the Ivanti EPMM Admin Portal in **Services > Sentry > Manage Certificate**.
2. If you uploaded a self-signed certificate, in **Settings > Sentry**,

Click on **View Certificate**.

Clicking on **View Certificate**, makes the Sentry certificate known to Ivanti EPMM.

If you have an Ivanti Tunnel deployment, push the Standalone Sentry certificate to devices.

3. If you have Ivanti Tunnel or AppTunnel deployments, you must re-push the Ivanti Tunnel VPN and AppConnect AppConfig configurations.

To re-push the configurations, remove then re-apply the configuration to labels.

Related topics

- For information on how to upload the Sentry certificate, see "Uploading Sentry certificates" on page 150.
- For information on how to push the Sentry certificate to devices see, *Using a Self-signed certificate with Standalone Sentry and Ivanti Tunnel* knowledge base article in the Support and Knowledge Base portal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Managing ActiveSync Email Devices

The following provide information about managing devices accessing the ActiveSync server through Sentry.

ActiveSync devices and Sentry

ActiveSync devices are devices accessing the ActiveSync server through Sentry. Sentry uses the ActiveSync protocol to communicate with the ActiveSync server and with ActiveSync devices to allow ActiveSync devices access to a user’s email, contacts, calendar, tasks, and notes. Sentry associates the user with the device accessing the ActiveSync server, and allows you to manage these associations.

ⓘ The terms ActiveSync devices, ActiveSync phones, and ActiveSync associations are used interchangeably and refer to the user and device accessing the ActiveSync server. Actions which specifically impact only the user or the device are called out.

ActiveSync associations

To display the users and the devices that connect to your ActiveSync server through Standalone, in Ivanti EPMM Admin Portal, go to **Devices & Users > ActiveSync**. Information displayed on this page is updated when Sentry syncs with Ivanti EPMM.

Each ActiveSync user (email account) on the device displays as a separate record in the **ActiveSync** page.

- If there are multiple email accounts on the device, then each User and Device association is listed in the ActiveSync Association view, but only the User registered on Ivanti EPMM for the device is listed in the All Devices view

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Typically, devices register with an Ivanti EPMM, which provides them with their email profile information. Once a device's email profile is set up, it can access the ActiveSync server.

When a device accesses the ActiveSync server, Sentry tries to match the device to a registered device on Ivanti EPMM. Typically, a successful match is made between the record on the ActiveSync page to the corresponding registered device on Ivanti EPMM. However, for some devices, no match is made, sometimes because MDM and ActiveSync do not report the same device information. In these cases, the status for the record in the ActiveSync and AppTunnel pages shows as Unregistered (Unlinked).
When the record is matched to the corresponding device on Ivanti EPMM, the status for the record shows as Registered(Linked).

- When an ActiveSync device registers with Ivanti EPMM, you can manage it using Ivanti EPMM. For example, you can apply security policies to a registered device.

However, using the ActiveSync view, you can take some actions on ActiveSync devices regardless of whether they are registered.
Notably, you can allow or block access to the ActiveSync server, assign an ActiveSync policy, or wipe the device.
We recommend applying ActiveSync actions (Wipe, Assign Policy, and Revert Policy in the ActiveSync page) to devices other than iOS, Android, and Windows Phone 8 devices.
Actions applied on a record in the ActiveSync page only impact the user associated with the device in that record. If the user is also available on another device, the user on that device is not impacted.
The wipe behavior differs depending on the platform. For example, for any Android device, the Email+ client does not support ActiveSync Wipe.
The Apply Policy and Revert Policy actions are applied to the device, not to the user.
Additional users on the Samsung native client display as unregistered in the ActiveSync page. To register the user, select the record, then click Link To to link to the corresponding device.

- ActiveSync devices that are registered, or are pending registration, automatically appear on the Devices view.

A device in the Users & Devices > Devices view is not necessarily shown in the ActiveSync view. For example, with Standalone Sentry, a registered device that has not accessed the ActiveSync server appears only in the Devices view, but not in the ActiveSync view.

If an ActiveSync device on the Devices view has an Active status, you can take all the actions on the device that the Devices view provides.

Sync interval with Ivanti EPMM

The default sync interval for Standalone Sentry is 12 hours.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

For Integrated Sentry, the information displayed on this page is updated after a successful periodic differential sync. The default interval for a periodic differential sync is 4 hours. You can configure the periodic differential sync in the Ivanti EPMM Admin Portal, **Services > Sentry > Preferences**. However, changes to the **Last Sync Time** for a record is not picked up in a periodic differential sync if it is the only field that was changed. For Integrated Sentry, the Last Sync Time, if it is not updated in a periodic differential sync, is updated after a full batched-sync. The default interval for a full batched-sync is one week.

Information displayed for ActiveSync associations

The following table describes the information displayed for ActiveSync associations in the Admin Portal in **Devices & Users > ActiveSync**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 27. INFORMATION DISPLAYED FOR ACTIVESYNC ASSOCIATIONS

Column	Description
DeviceID	The DeviceID for the device.
User	The device user.
Number	The device number.
Phone	The device model.
OS	The device platform.
Status	Indicates whether the device is registered with Ivanti. • When a record is associated with a registered device on Ivanti EPMM, the status displays as Registered(Linked). • When a record is not associated with a registered device on Ivanti EPMM, the status displays as Unregistered (Unlinked). Use the **Link To** feature to link the record to the corresponding registered device.
Sync Status	Indicates whether ActiveSync access for the device is Allowed or Blocked.
First Sync Time	For Integrated Sentry, the First Sync Time displays the time stamp for the first successful synchronization of data from the Exchange server. For Ivanti Standalone Sentry, the First Sync Time displays the time stamp when the device is first reported by Sentry to Ivanti EPMM as a new device.
Last Sync Time	Indicates the last time the device tried to access the ActiveSync server. The **Last Sync Time** does not indicate whether access to the ActiveSync server was successful or not. Therefore, the last sync time on the ActiveSync server may be different than what is recorded by Standalone Sentry. For Standalone Sentry, the Last Sync Time is updated only if Standalone Sentry detects traffic between the device and the ActiveSync server. For Integrated Sentry, the Last Sync Time is updated only after a full batched sync.
Mailbox ID	Displays the ID for the synchronized mailbox as defined in ActiveSync.
Domain	Indicates whether the device connects via Integrated Sentry or Standalone Sentry.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

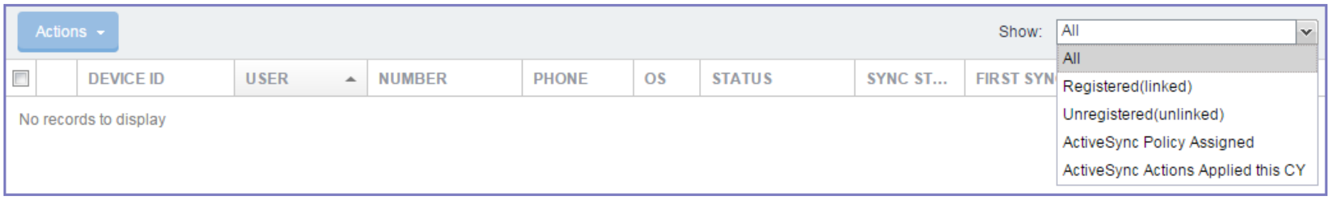
For iOS 8, when a device is wiped, the device gets a new device ID. When the same device re-registers with Ivanti EPMM and syncs with Exchange a new entry is created for the device in the ActiveSync page. The old entry for the device, which has old device ID, is blocked. The old entry in the ActiveSync page is not associated to the device when it re-registers.

Additional users on the Samsung native client display as unregistered in the ActiveSync page. To register the user, select the record, then click Link To to link to the corresponding device.

Filter options for the ActiveSync associations list

To filter the devices displayed in the **ActiveSync** page in the Admin Portal (**Devices & Users > ActiveSync**), select one of the criteria in the drop-down list for **Show**.

FIGURE 1. FILTER OPTIONS FOR THE ACTIVESYNC ASSOCIATIONS LIST



No records to display

TABLE 28. FILTER OPTIONS FOR THE ACTIVESYNC ASSOCIATION LIST

Item	Description
Registered(linked)	Displays records that are associated with a registered device on Ivanti EPMM.
Unregistered(unlinked)	Displays records that are not associated with a registered device on Ivanti EPMM.
ActiveSync Policy Assigned	Displays associations with device to which an ActiveSync policy is manually assigned.
ActiveSync Action Applied in CY	Displays associations with device on which an ActiveSync action is applied in the calendar year.

Displaying more information for an ActiveSync association

To display more information for an ActiveSync association:

1. In the **ActiveSync** page, select an ActiveSync record.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

The **ActiveSync Details** pane on the right displays additional information about the record.

2. Click the arrow for a category to display additional details.

Information available in the ActiveSync Details pane

The following table describes the information available in the ActiveSync details pane in the Admin Portal.

TABLE 29. INFORMATION IN THE ACTIVESYNC DETAILS PANE

Label	Description
User	The user (email account) accessing the ActiveSync server.
Phone	The device number and model.
Device Details	Additional details received from the device.
Mailbox Details	The ActiveSync policy applied to the mailbox. Redirect URL, if there is a redirect URL, to which the device is redirected.
Comment	Comments you may have added to this record.

Taking Actions on ActiveSync associations

Actions applied on a record in the ActiveSync page only impact the user associated with the device in that record. If the user is also available on another device, the user on that device is not impacted.

Allow, Block, and Wipe actions override Ivanti EPMM's automatic decision-making about a device's ability to access the ActiveSync server. For more information, see "Assign policy" on page 161.

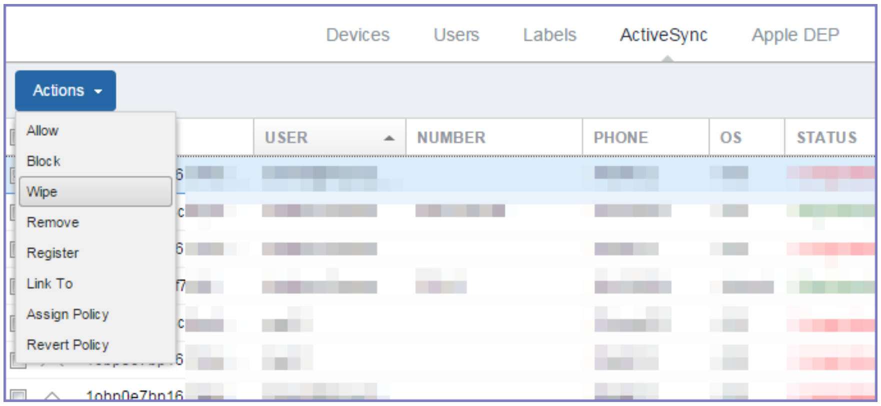
Ivanti recommends applying ActiveSync actions to devices other than iOS, Android, and WP8 devices. Wipe, Assign Policy, and Revert Policy are ActiveSync actions. The Assign Policy and Revert Policy actions are applied to the device, not to the user.

Procedure

1. In the Admin Portal, go to **Devices & Users > ActiveSync.**

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. ACTIVESYNC ASSOCIATION ACTIONS



2. Select an ActiveSync record.
3. Click **Actions**, then click one of the following:
   - **Allow**
   - **Block**
   - **Wipe**
   - **Register**
   - **Remove**
   - **Link To**
   - **Assign Policy**
   - **Revert Policy**
4. Enter a note in the pop-up dialog.
5. Click the ActiveSync action button in the pop-up dialog.

Related topics

- "Allow" on the next page.
- "Block" on the next page
- "Wipe" on the next page
- "Register" on the next page
- "Remove" on the next page
- "Linking an ActiveSync device to a managed device" on page 161
- "Assign policy" on page 161
- "Revert policy" on page 161

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Allow

The Allow action allows:

- blocked ActiveSync devices to access the ActiveSync server.
- the ActiveSyncy association to access the ActiveSync server, regardless of possible security policy violations.

Block

The Block action blocks the selected ActiveSync association from accessing the ActiveSync server even if it is not in violation of its security policy.

Wipe

Wiping an ActiveSync phone sends an ActiveSync Wipe command to the phone, which removes all data from the phone, returning the phone to factory defaults. Once you wipe a phone, its status changes to **Wiped**, and the only valid action you can apply is **Remove**.

The wipe behavior differs depending on the platform. For example, for any Android device, the Email+ client does not support ActiveSync Wipe.

Returning the phone to factory defaults removes all data. Once a wipe has started, do not restart your phone. Interfering with the wipe process can render your phone non-functional.

ⓘ The device is wiped only when it attempts to sync, or the user takes an action. For example, the device is wiped when the device user attempts to send an email.

Register

Registering an ActiveSync phone with Ivanti enables device management and intelligence functions for the phone. See “ActiveSync device registration” in the Ivanti EPMM Device Management Guide.

Remove

Removing an ActiveSync device removes the association between the phone and the ActiveSync mailbox. All information about the phone is removed, including any previously configured Allow, Block or Wipe commands.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

For more information about using Remove, see "Assign policy" below.

Linking an ActiveSync device to a managed device

In most cases, Ivanti automatically matches the device record on the ActiveSync server to the corresponding device record on Ivanti EPMM. If this link does not happen automatically, you can use the **Link To** feature to link a device in the **ActiveSync** page to a device in the **Devices** page to establish this match.

Procedure

1. Select the device in the **ActiveSync** page.
2. Click **Actions > Link To**.
3. Select the corresponding device from the popup.

If the corresponding device is already linked to another ActiveSync entry, you will be presented with the option to either **Replace** the previous association with the selected device, or **Duplicate** to additionally associate the selected device.

4. Click **Link To**.

Assign policy

You have to manually apply an ActiveSync policy to a device. If an ActiveSync policy is not applied to a device, the **Default ActiveSync Policy** behavior configured in **Settings >Sentry > Preferences** is applied to the Sentry interaction with the ActiveSync server.

Apply this action only to devices other than iOS, Android, and WP8 devices.

Revert policy

Reverting an ActiveSync policy reverts the device to the Default ActiveSync Policy behavior configured in **Services > Sentry > Preferences**. The default behavior is applied only when the device engages in an ActiveSync Provision.

Overriding and re-establishing Ivanti EPMM management of a device

Ivanti EPMM automatically makes decisions to perform allow, block, or wipe actions based on the following:

- the device’s security policy
- whether the maximum number of devices per mailbox has been exceeded

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- whether you specified to auto block unregistered devices

However, you can override Ivanti EPMM's management by manually selecting **Allow, Block,** or **Wipe**.

Reestablishing Ivanti EPMM management

Once you select the **Allow, Block,** or **Wipe** for the device, Ivanti EPMM no longer automatically makes these decisions. You can reestablish Ivanti EPMM management of the device by removing the device from the **ActiveSync** page. The next time the device accesses its email, Ivanti EPMM adds the device back to the view, and once again manages the device based on its security policy.

Procedure

1. In the Admin Portal, go to **Devices & Users** > **ActiveSync**.
2. Select the ActiveSync association, then click **Remove**.

Ivanti EPMM removes the device from the **ActiveSync** page.

Determining if a device was recently blocked or allowed

You can determine if a device was recently blocked or allowed, and if it was a manual or automatic action.

Procedure

1. In the Admin Portal, go to **Log** > **Browse All**.
2. Look for **Block** or **Reinstate** (which means allowed) in the **Action** column.

The message column indicates if the action was due to the security policy. If the action was manual, the message column is either empty, or contains a note added by the administrator who performed the manual action.

Multiple ActiveSync email accounts on a registered device

Ivanti Standalone Sentry and Integrated Sentry support multiple email accounts on the same device for the following use cases:

- The device user requires access to another user's email account.

- The device user is a member of a group and requires access to the group's email account.

- ActiveSync server: The email accounts must exist on the same type of ActiveSync server. Ivanti Standalone Sentry does not support syncing email accounts that are on different types of ActiveSync servers, for example, an email account on a Gmail server and another account on an Microsoft Exchange server, on the same device.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- Security policy: Since security policies are applied to the device, if the device is not in compliance, all ActiveSync email accounts on the device are blocked. If the same email account is available on a second device that is in compliance, the user of the second device continues to have access to the email account.

Whether the security policy or the ActiveSync policy takes precedence depends on the device. There are no changes to this behavior.

- ActiveSync policy: We recommend applying the an ActiveSync policy to only one email account on the device. If multiple email accounts are configured on a device and a different ActiveSync policy is applied to each account, it is difficult to determine which ActiveSync policy is applied to an email account.

- Device: The device must be registered on Ivanti EPMM.

- For supported devices, see Multi Mailbox in the Email Client Support Matrix.

- User: The user of the email account, must be registered on Ivanti EPMM. If the user is not registered, do one of the following:

- Create a local user account for the user. For instructions on how to add a local user account, see “Adding Local Users in Admin Portal” in the Ivanti EPMM Device Management Guide.
- Alternately, log into the User Portal with the LDAP credentials for the user. For more information on how to log into User Portal, see “User Portal” in the Ivanti EPMM Device Management Guide.

- Android devices: You can apply up to two Exchange settings for each device. The device must be running Mobile@Work when it receives the configuration.

- On the device, both mailboxes appear in a single email app. The email app is determined by 1) the email app’s priority as specified in the **Exchange** setting’s **Exchange App Priority**, and 2) the email app’s availability on the device. For example, if both Samsung Native Email and Email+ are available on the device, the app with the highest priority is used.

Options > Email Status is not supported for multiple ActiveSync accounts.

Methods for adding additional email accounts

You can add additional ActiveSync email accounts in one of the following ways:

- "Pushing additional email account to the device" on the next page.

- "Manually add email account to device" on page 166.

To access the email account, the device user will require the password for the email account.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Pushing additional email account to the device

In this method for adding additional email accounts to a registered device, no actions are required by the device user. However, this method requires modifying the attributes for the device user in Active Directory.

Before you begin

Manually modify the ExtensionAttributes for the device user in Active Directory. For extensionAttribute1 enter the username of additional email account, and for extensionAttribute2 enter the email address of the additional email account.

For detailed instructions see the *How to Add Multiple EAS Accounts to a Single Device* knowledge base article.

Overview of steps on Ivanti EPMM

1. "Mapping the custom attributes created in AD to LDAP settings" below.
2. "Sync with LDAP." below.
3. "Create new Exchange setting" below.
4. "Create new label" on the next page.
5. "Apply Exchange setting to label" on the next page.
6. "Apply device user to label" on the next page.

Procedure

1. Mapping the custom attributes created in AD to LDAP settings

In the Admin Portal, go to **Settings** > **LDAP**.

Select the LDAP setting and click the edit icon.

For **Custom 1**, enter **extensionAttribute1**. For **Custom 2**, enter **extensionAttribute2**.

Save the edited LDAP setting.

2. Sync with LDAP.

In the Admin Portal, go to **Users & Devices** > **Users**.

Click **Resync With LDAP**.

Wait for the LDAP sync to complete.

To verify, click on the **System Manager** link.

In the system manger, go to **Troubleshooting** > **Service Diagnostic** > **LDAP Sync History**.

3. Create new Exchange setting

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

In the Admin Portal go to **Policies & Configs > Configurations**.

Click **Add New > Exchange**.

Enter the information requested.

In the ActiveSync **User Name** field, enter $USER_CUSTOM1$.

In the ActiveSync **User Email** field, enter $USER_CUSTOM2$.

Except for the ActiveSync UserName and ActiveSync User Email fields, you may want to configure the new Exchange setting with the same information you used for the Exchange profile you are currently pushing to the devices.

Click **Save**.

4. Create new label

In the Admin Portal go to **Users & Devices > Labels**.

Click **Add Label**.

Enter the information requested.

Click **Save**.

5. Apply Exchange setting to label

In the Admin Portal go to **Policies & Configs > Configurations**.

Select the Exchange setting.

Click **More Actions > Apply to Label**.

In the **Apply To Label** dialog, select the label you created.

Click **Apply**.

6. Apply device user to label

In the Admin Portal, go to **Users & Devices > Devices**.

Select the device to which the email account will be added.

Click **Actions > Apply** to Label.

In the **Apply To Label** dialog, select the label you created.

Click **Apply**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

The email account is pushed to the device when it syncs.

No actions are required by the device user.

To access the email account, the device user requires the password for the email account.

Related topics

For information on how to create an Exchange setting, see “Exchange settings” in the Ivanti EPMM Device Management Guide.

Manually add email account to device

To manually add the email account, the device user will require the following information:

- The username and password for the ActiveSync email account.
- The Sentry FQDN (or the external name of your Standalone Sentry).

You do not need to make any changes to AD or Ivanti EPMM.

When setting up the additional email account on the device, for the server address, enter the Standalone Sentry FQDN or the external name of your Standalone Sentry.

If your Standalone Sentry is set to Auto Block Unregistered(unlinked) Devices

In the Admin Portal, **Services > Sentry > Preferences**, if **Auto Block Unregistered(unlined) Devices** is set to **Yes**, you may get a verification failure when you are setting up the additional email account. If you do, save the settings anyway.

After adding the account on the device, go to the Admin Portal, **Devices & Users > ActiveSync**. Search for the username of the account you just added, select the entry, and click **Allow**.

Allowing Windows 7 devices to sync

Windows 7 devices cannot register with Ivanti EPMM, because Windows 7 does not have device management features. However, these devices sync using Exchange ActiveSync and are managed using ActiveSync policies.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Before you begin

If your Sentry uses a self-signed certificate, from a browser download the Sentry self-signed certificate and its signing certificate, the CA certificate. The specific steps differ slightly for each browser type. For information on how to download the Sentry self-signed certificate, see "Downloading the Sentry self-signed certificate" on the next page.

Overview of steps

1. "On Ivanti EPMM, set Auto Block Unregistered Devices to No." below
2. "Install the self-signed certificate and its signing certificate, the CA certificate on the device." below
3. "Configure the Exchange ActiveSync account on the device." below

Procedure

1. On Ivanti EPMM, set **Auto Block Unregistered Devices** to **No**.

In the Admin Portal, navigate to **Services > Sentry** > **Preferences**.

For **Auto Block Unregistered (unlinked) Devices**, select **No**.

The default setting for **Auto Block Unregistered (unlinked) Devices** is set to **No**.

2. Install the self-signed certificate and its signing certificate, the CA certificate on the device.

If your Sentry has a certificate signed by a third-party CA, skip this section and go to "Configure the Exchange ActiveSync account on the device." below.

Email the two certificates (self-signed and CA) to an email account on the device, for example, a GMail or a Yahoo account.

On the device, tap on the attachments to download.

Tap the shield icons to install the certificates.

Go to "Configure the Exchange ActiveSync account on the device." below.

3. Configure the Exchange ActiveSync account on the device.

On the device, tap **Settings > email + accounts > add an account > advanced setup**.

Enter your email address and Password, then tap **Next**.

Tap **Exchange ActiveSync** as the email account type.

In the Domain field, enter the domain of the email server.

In the Server field, enter *sentryhostname*, where *sentryhostname* is the fully-qualified domain name for Sentry.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Check **Server requires encrypted (SSL) connection**.

Tap **sign in**.

The device begins to sync.

Downloading the Sentry self-signed certificate

You can download the download the Sentry self-signed from a browser. The steps differ slightly between browsers. The following sections provide the steps to download the Sentry self-signed certificate and its signing certificate, the CA certificate, using the Chrome browser.

- "Downloading the Sentry self-signed certificate on a Mac OSX using Chrome" below
- "Downloading the Sentry self-signed certificate on Windows using Chrome" below

Downloading the Sentry self-signed certificate on a Mac OSX using Chrome

These steps are specific to the Chrome browser. You may want to download the self-signed certificate if you are registering a Windows 7 device to Ivanti EPMM using ActiveSync and Sentry uses a self-signed certificate.

Procedure

1. Navigate to **https://***sentryhostname*, where *sentryhostname* is the Sentry fully-qualified domain name.
2. Click on the Https padlock icon in the address bar.
3. Click **Certificate Information**.
4. Click the signing certificate (CA), then drag the certificate icon from the panel to your desktop.
5. Click the self-signed certificate, then drag the certificate icon from the panel to your desktop.

Related topics

"Allowing Windows 7 devices to sync " on page 166.

Downloading the Sentry self-signed certificate on Windows using Chrome

These steps are specific to the Chrome browser. You may want to download the self-signed certificate if you are registering a Windows 7 device to Ivanti EPMM using ActiveSync and Sentry uses a self-signed certificate.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. Navigate to **https:**//*sentryhostname*, where *sentryhostname* is the Sentry fully-qualified domain name.
2. Click on the Https padlock icon in the address bar.
3. Click **Certificate information**.
4. Click the **Details** tab.
5. Click **Copy to File**...
6. The Certificate Export Wizard appears.
7. Click **Next**.
8. Select the format you want to use as **Base-64 encoded X.509 (.CER)**, click **Next**.
9. Click **Browse** to navigate to the Desktop to save the file.
10. Enter a name for the file and click **Save**, then **Next**, then **Finish**.

Other formats are recognized by Windows Phone 7 as valid certificates, but other formats will not work with an Exchange ActiveSync account.

11. Click the **Certification Path** tab.
12. Select the signing certificate (CA certificate).
13. Click the **Details** tab.
14. Click **Copy to File...**
15. The Certificate Export Wizard appears.
16. Click **Next**.
17. Select the format you want to use as **Base-64 encoded X.509 (.CER)**, then click **Next**.
18. Click **Browse** to navigate to the Desktop to save the file.
19. Enter a name for the file and click **Save**, then **Next**, then **Finish**.

Related topics

"Allowing Windows 7 devices to sync " on page 166.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Managing App Tunnels

The following provide information about working with app tunnels:

Manually blocking the AppTunnel feature on a device

You can manually block the AppTunnel feature on a device for apps using AppTunnel as well as apps using Tunnel. The authorized apps remain authorized, but the apps will no longer be able to access the web sites configured to use the AppTunnel feature.

Procedure

1. Go to **Devices & Users > Devices**.
2. Select a device.
3. Select **Actions > More Actions > Block App Tunnels**.
4. Add a note.
5. Click **Block AppTunnels**.

Unblocking the AppTunnel feature on a device

If you had blocked the AppTunnel feature on a device, you can then unblock the AppTunnel feature.

Procedure

1. Go to **Devices & Users > Devices**
2. Select a device.
3. Select **Actions > More Actions > Allow App Tunnels**.
4. Add a note.
5. Click **Allow AppTunnels**.

View app tunnels details

Once an app tunnel is established, you can view the AppTunnel details in the App Tunnels page.

To view app tunnels, in the Admin Portal, go to **Apps > App Tunnels**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

The following information is displayed:

TABLE 30. APPTUNNEL DETAILS

Column	Description
Application	The app bundle ID. For Docs@Work, the app name is displayed.
User	The app user.
Model	The device UUID. The device UUID allows you to distinguish between app tunnels created with the same user and app but from different devices.
Status	The status of the device.
State	The app tunnel state. The state can be Allow or Block.
Version	The app tunnel headers version that the device uses to talk to Ivanti Standalone Sentry. V1 indicates the AppTunnel version that supports HTTP and HTTPS traffic only. V2 indicates the AppTunnel version that supports HTTP, HTTPS, TCP, and IP traffic.
Service	Service name of the app tunnel.
Creation Time	The time when the app tunnel was created.
Last Connected	The last time the device using the tunnel synced with Ivanti Standalone Sentry.

Taking actions on app tunnels

You can allow, block, or remove an app tunnel in the Admin Portal.

Procedure

1. In the Admin Portal, go to **Apps > App Tunnels**.
2. Select the app tunnel you wish to take action on.
3. Click on one of the actions described in the following table.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 31. APPTUNNEL ACTIONS DESCRIPTIONS

Action	Description
Allow	Permits the app to access backend resource(s) through a Ivanti Standalone Sentry.
Block	Prohibits the app from accessing the backend resource(s) through a Standalone Sentry.
Remove	Deletes the app tunnel information. After a **Remove**, Sentry will not have any memory of the app tunnel. When the user on the device uses the app, a new a app tunnel is established. Remove is generally used for troubleshooting purposes.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry Settings

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

Overview of Ivanti Standalone Sentry settings

The settings tab in the Ivanti Standalone Sentry System Manager contains links for configuring Ivanti Standalone Sentry. Ivanti recommends allowing HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for Ivanti Standalone Sentry System Manager and must have strictly controlled access. To log in to the Sentry System Manager, go to https://*fully_qualified_hostname*:8443.

TABLE 32. CONFIGURATION LINKS IN THE SETTINGS TAB

Setting	Description
Network: Interfaces	Change physical interface settings. Add VLAN interfaces. Change VLAN interfaces.
Network: Routes	Change the default gateway. Route through different gateways.
DNS and Hostname	Change DNS servers.
Static Hosts	Edit the host list for the Standalone Sentry.
Date and Time (NTP)	Change the time source used by the Standalone Sentry.
CLI	Change the Enable Secret set during installation. Enable or Disable ssh access. Change ssh settings.
Splunk	Configure Splunk server.
Syslog	Configure Syslog servers.
Log Upload	Upload Sentry log files to Technical Support or other support provider.
SNMP	Configure SNMP servers.
Email Settings	Configure SMTP servers.
Services	Enable or Disable Sentry services.
Services: Sentry	Allow or block New device access when UEM is unreachable.
Services: Sentry: Cipher Suites & Protocols	Customize Cipher Suites and Protocols settings.

Interfaces

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

- physical and VLAN interfaces
- static routes

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Physical and VLAN interface fields are not editable for a Ivanti 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 Ivanti EPMM System Manager to the physical NIC port in the M2600 appliance. The six Gigabit Ethernet interfaces are available only on an M2600 appliance.

TABLE 33. PHYSICAL INTERFACE MAPPING TO M2600 NIC PORTS

Physical interface	M2600 NIC port
GigabitEthernet1	I - eth0 (NIC-3)
GigabitEthernet2	J - eth1 (NIC-4)
GigabitEthernet3	K- eth2 (NIC-5)
GigabitEthernet4	L- eth3 (NIC-6)
GigabitEthernet5	C- eth4 (NIC-1)
GigabitEthernet6	D- eth5 (NIC-2)

Changing physical interfaces

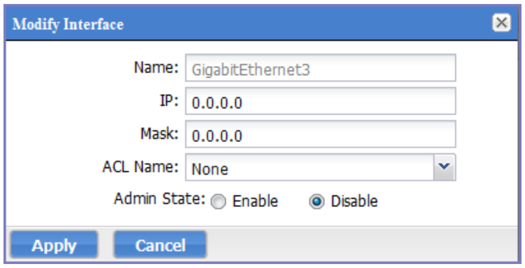
You can change the physical interfaces for Ivanti Standalone Sentry in the Sentry System Manager.

Procedure

1. Click the interface name.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. MODIFY PHYSICAL INTERFACES



Name: GigabitEthernet3

IP: 0.0.0.0

Mask: 0.0.0.0

ACL Name: None

Admin State: ○ Enable ● Disable

2. Change any or all of the following fields:

Field	Description
IP	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.
Mask	Enter the netmask of the physical network interface.
ACL Name	Select an Access Control List for this interface.
Admin State	To enable this interface for use with the system, click Enable. To temporarily prevent use of this interface with the system, click Disable.

3. Click **Save**.

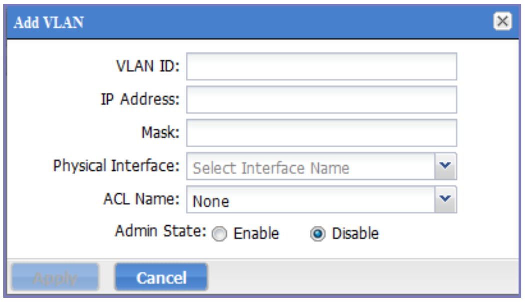
Adding VLAN interfaces

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 Ivanti Standalone Sentry System Manager.

Procedure

1. Click **Add VLAN**.

FIGURE 2. ADDING VLAN



VLAN ID:

IP Address:

Mask:

Physical Interface: Select Interface Name

ACL Name: None

Admin State: ○ Enable ● Disable

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

2. Use the following guidelines to complete the configuration:

Field	Description
VLAN ID	Specify a number between 2 and 4094.
IP Address	Enter the IP address for this VLAN interface.
Mask	Enter the netmask for this VLAN interface.
Physical Interface	Select the physical interface that corresponds to this VLAN interface.
ACL Name	Select an Access Control List for this interface. See "Access Control Lists" on page 235.
Admin State	To enable this interface, click Enable. To temporarily suspend use of this VLAN, click Disable.

3. Click **Save**.

Deleting a VLAN interface

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

Procedure

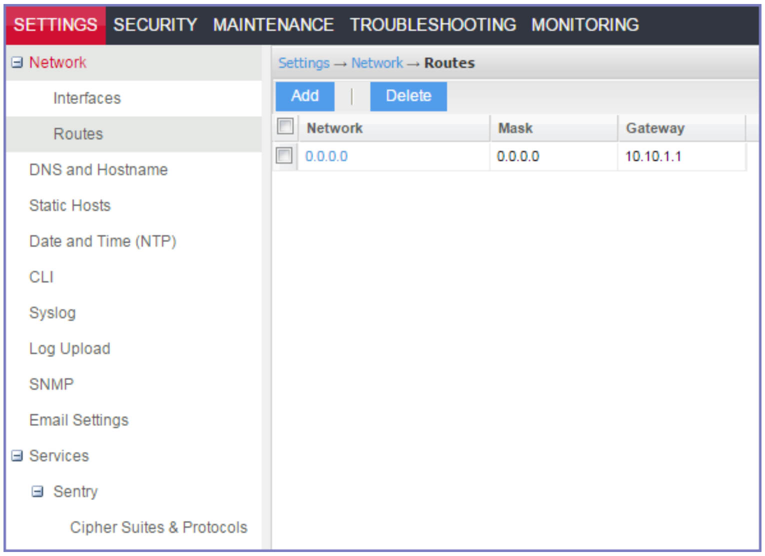
1. Select the VLAN you want to remove.
2. Click **Delete VLAN**.

Routes

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. STANDALONE SENTRY ROUTES



□	Network	Mask	Gateway
□	0.0.0.0	0.0.0.0	10.10.1.1

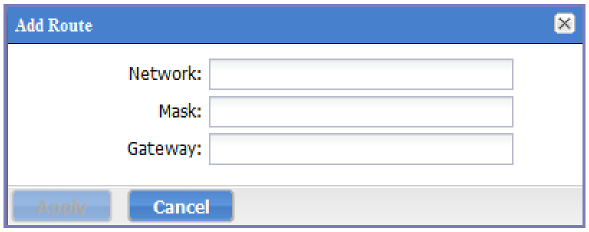
Adding network routes

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

Procedure

1. In the Ivanti 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:

Field	Description
Network	Enter the network IP address.
Mask	Enter the subnet mask.
Gateway	Enter the IP address for the gateway.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. Click **Save**.

Deleting network routes

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

Procedure

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

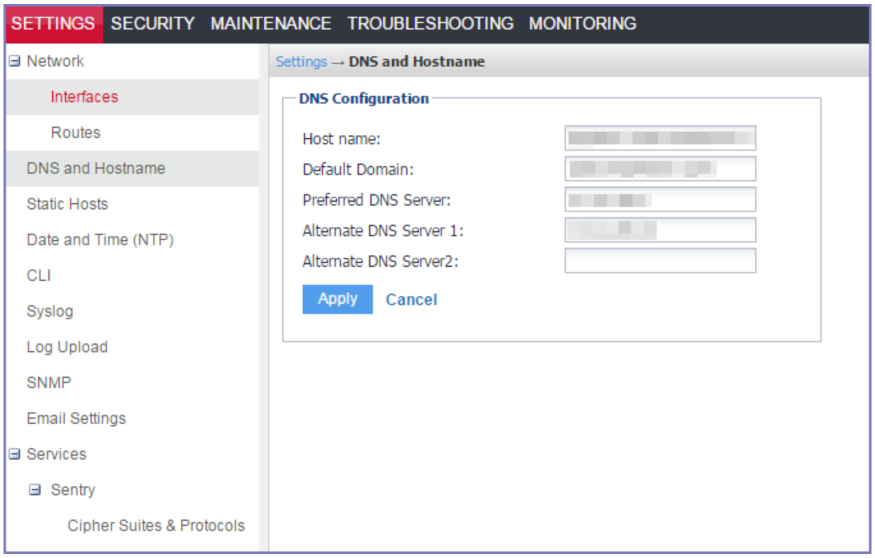
DNS and Hostname

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

For an Ivanti Standalone Sentry installed on Microsoft Azure and AWS, the DNS and hostname fields are automatically assigned by the infrastructure and those fields are not editable.

FIGURE 1. DNS AND HOSTNAME



DNS Configuration

Host name: [redacted]
Default Domain: [redacted]
Preferred DNS Server: [redacted]
Alternate DNS Server 1: [redacted]
Alternate DNS Server2:

The following table describes the fields for DNS and hostname.

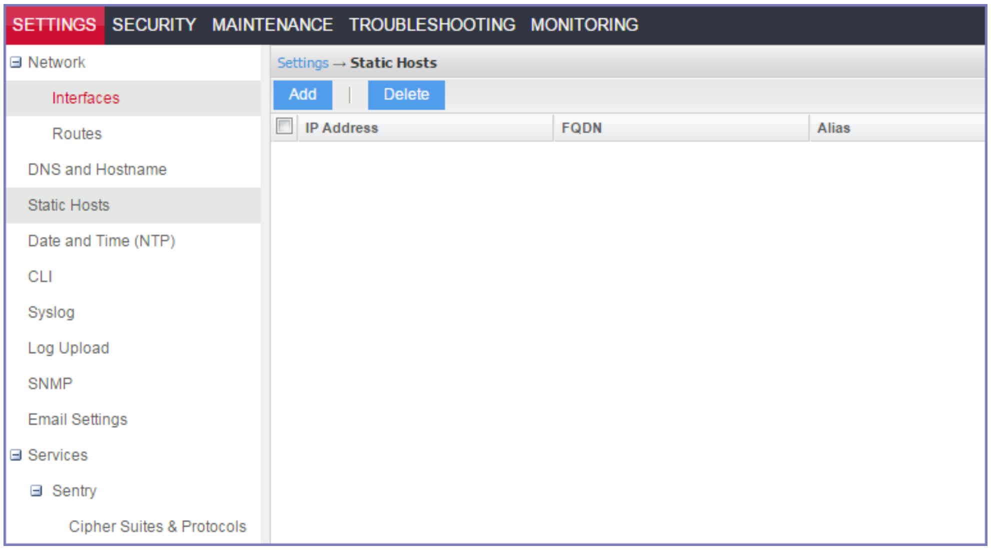
TABLE 34. DNS AND HOSTNAME FIELD DESCRIPTION

Field	Description
Host name	Specify the fully-qualified host name for the appliance.
Default Domain	Specify the default domain for the appliance.
Preferred DNS Server	Specify the IP address of the primary DNS server to use.
Alternate DNS Server 1	Specify the IP address of an optional alternate DNS server.
Alternate DNS Server 2	Specify the IP address of an optional alternate DNS server.

Static Hosts

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

FIGURE 1. STATIC HOSTS



Adding hosts

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

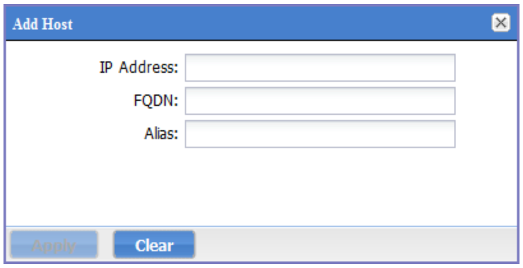
Procedure

1. In the Ivanti Standalone Sentry System Manager go to **Settings > Static Hosts.**

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

2. Click the **Add** button.

FIGURE 2. ADDING STATIC HOSTS



3. Use the following guidelines to complete the displayed fields:

Field	Description
IP Address	The IP address for the host you are adding.
FQDN	The fully-qualified domain name for this host, as in myserver.mycompany.com.
Alias	The alias for this host. Up to 29 aliases are allowed.

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 Ivanti 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 Ivanti Standalone Sentry System Manager in **Settings** > **Static Hosts**.

Procedure

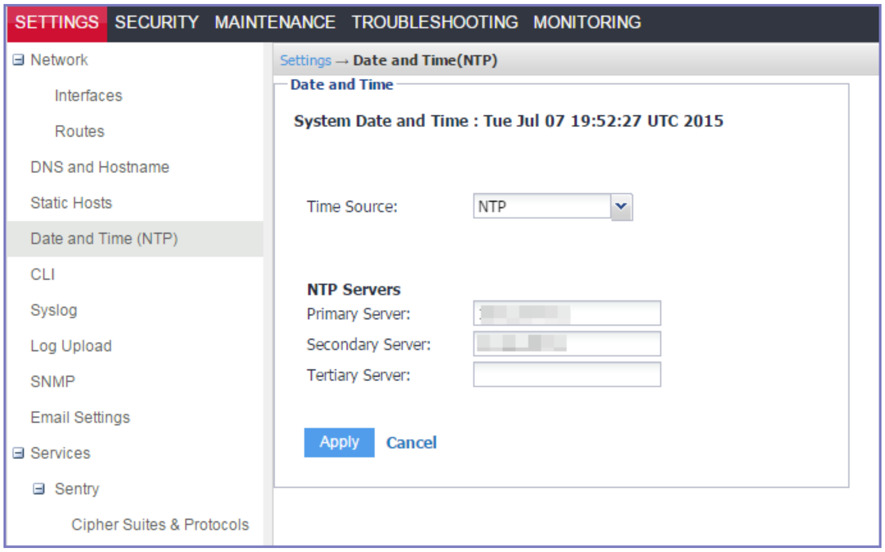
1. In the **Static Hosts** screen, select the host to be deleted.
2. Click **Delete**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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.

FIGURE 1. DATE AND TIME (NTP)



System Date and Time : Tue Jul 07 19:52:27 UTC 2015

Time Source: NTP

NTP Servers

Primary Server: [redacted]

Secondary Server: [redacted]

Tertiary Server:

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 35. DATE AND TIME (NTP)

Field	Description
Time Source	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.
If you select NTP	
Primary Server	Specify the IP address or fully-qualified host name for the NTP server to use.
Secondary Server	Specify the IP address or fully-qualified host name for the first failover NTP server to use.
Tertiary Server	Specify the IP address or fully-qualified host name for the second failover NTP server to use.
If you select Local	
Date	Enter the current date.
Time	Enter the current time.

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".

The following table describes the CLI settings.

TABLE 36. CLI FIELD DESCRIPTIONS

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Splunk

You can configure a Splunk entry Ivanti 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 Ivanti Standalone Sentry

Following is an overview of the steps for setting up Splunk on Standalone Sentry:

1. "Enabling the Splunk forwarder service in Ivanti Standalone Sentry" below.
2. "Adding a Splunk receiver entry in Ivanti Standalone Sentry" below.
3. "Configuring Ivanti Standalone Sentry data to export to Splunk" on the next page.
4. "Tasks in Splunk server to set up Ivanti Standalone Sentry" on the next page

Enabling the Splunk forwarder service in Ivanti 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 Ivanti 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 Ivanti Standalone Sentry" below.

Adding a Splunk receiver entry in Ivanti Standalone Sentry

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

Procedure

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Fields	Description
Splunk Receiver	Add the IP address or the hostname of your Splunk Enterprise Server.
Port	Add the port of your Splunk Enterprise Server.
Enable SSL	(Optional) Click the check box to enable SSL.

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

Next steps

Go to "Configuring Ivanti Standalone Sentry data to export to Splunk" below.

Configuring Ivanti Standalone Sentry data to export to Splunk

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

Procedure

1. SSH to Ivanti 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 Ivanti Standalone Sentry" below.

Related topics

See "Log representation and format" on page 218 for the representation and the format of the data captured in audit and health logs.

Tasks in Splunk server to set up Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 37. SYSLOG FIELDS DESCRIPTION

Field	Description
Server	Enter the IP address or host name for the remote log server.
Port	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.
Protocol	Select UDP or TCP. Select UDP or TCP, depending on whether your syslog server is set up to receive UDP or TCP data.
Facility Type	Select the appropriate facility type to select the logs to report to syslog server. **General**: 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 **Troubleshoot > Service Diagnosis** in the Sentry System Manager. **Audit**: Select to send audit logs. **Health Monitor**: Select to send health monitoring logs.
Log Level	Select a log level from the drop down list. The log level is listed based on the priority and severity of the log message. **Emergency** **Alert** **Critical** **Error** **Warning** **Notice** **Info** **Debug** 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 **Audit** and **Health Monitor**, **Info** is the only log level available. ⓘ If the log level configured for the syslog server is higher than the log level configured on Sentry, Sentry only sends Alert/Error/Warning messages to the syslog server.
Admin State	Select **Enable** from the dropdown list to apply these settings to your current configuration. Select **Disable** to suspend use of the configured log server.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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:

Server: Enter the IP address of Monitor.

Port: Use the default port 514.

Protocol: Select the desired protocol.

Facility Type: Select General.

Only General is supported.

Log Level: Select the desired log level.

Admin State: Select **Enable**.

4. Click **Apply**.

Uploading logs

Use the Log Upload screen to set up optional default sites to which logs are uploaded. You can set up a default upload site for HTTPS and SFTP.

Procedure

1. Select **Settings > Log Upload**.
2. Fill out the forms for SFTP Server Configuration and HTTPS Server Configuration:
   - **Host/IP** or URL
     For Host/IP, enter the server name. For example, support.mobileiron.com.
     For URL, enter the FQDN. For example, https://support.mobileiron.com.
   - **User Name**
   - **Password**

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- **Confirm Password**

3. Click **Apply**.

After you click **Apply**, a **Change Password** link appears. If the login credentials change later for the servers, click the link to update the passwords to the new credentials.

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" on the next page to which Sentry sends SNMP traps.

2. "Enabling the SNMP service with the v3 protocol" on page 193 from whom Sentry accepts requests.

3. "Enabling the SNMP service with the v2c protocol" on page 196 between Sentry and your SNMP server.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti Standalone 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 **Add SNMP Trap Receiver** 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 38. FIELDS AND DESCRIPTIONS IN THE ADD SNMP TRAP RECEIVER WINDOW

Fields	Description
Server	Enter the IP address or server name for your SNMP trap receiver. For example: trapreceiver.myCompanyDomain.com
Port	By default, port 162 is configured. Edit this field if you are using a different port.
Community	Enter the string which names the SNMP community on your SNMP trap receiver.
Version	Sentry sends SNMP traps using SNMP protocol v2c.
Admin State	Select **Enable** to enable the SNMP service for this SNMP server.

Editing a trap receiver

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In the Ivanti 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, navigate to **Settings > SNMP** in the Ivanti Standalone Sentry System Manager.

Procedure

1. In the Ivanti 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 Ivanti Standalone Sentry accepts requests. In addition, you can enable or disable sending traps to any configured SNMP trap receiver.

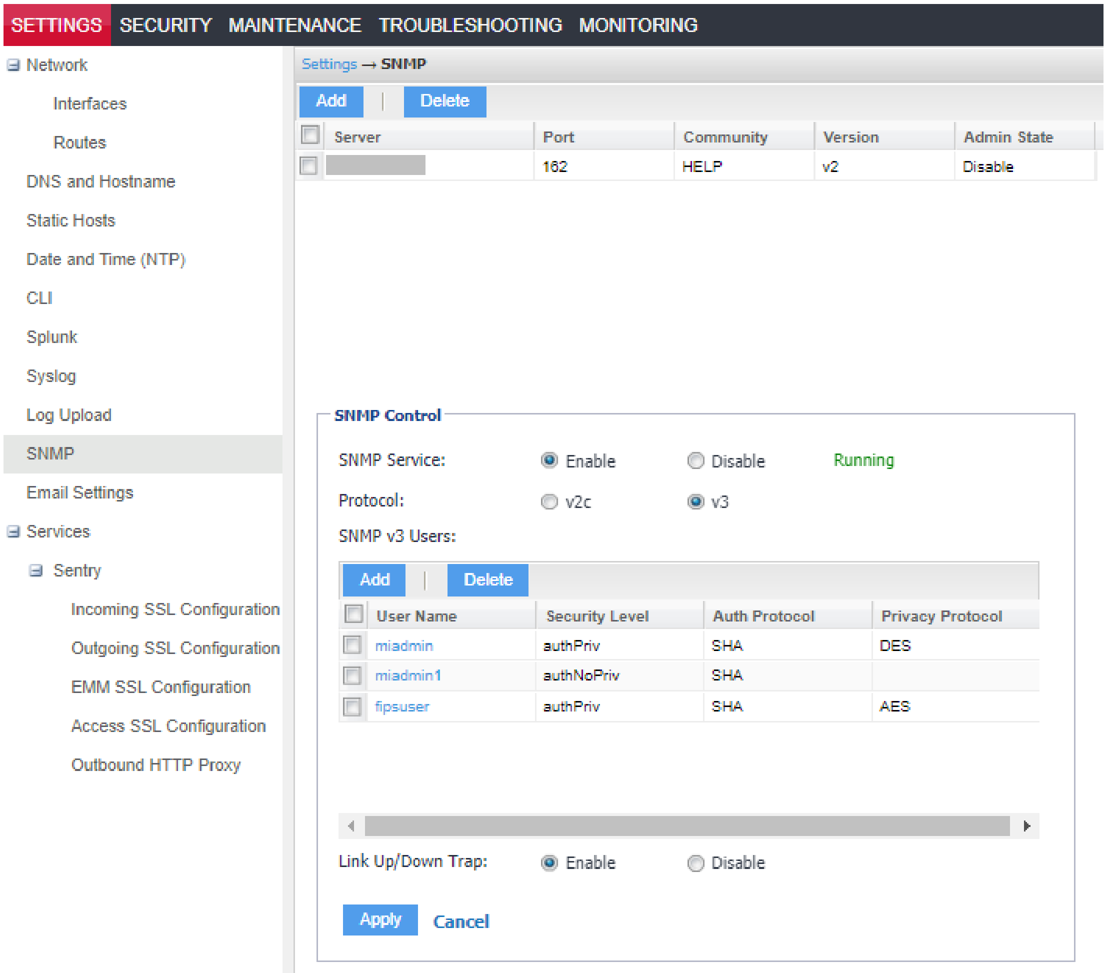
Procedure

1. Log into Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. Go to the **Protocol** option and verify that **v3** is selected.
   The v3 option is selected, by default.

FIGURE 1. SNMP SERVICE



□	Server	Port	Community	Version	Admin State
□	[redacted]	162	HELP	v2	Disable

SNMP Control

SNMP Service: ● Enable ○ Disable Running

Protocol: ○ v2c ● v3

SNMP v3 Users:

□	User Name	Security Level	Auth Protocol	Privacy Protocol
□	miadmin	authPriv	SHA	DES
□	miadmin1	authNoPriv	SHA	
□	fipsuser	authPriv	SHA	AES

Link Up/Down Trap: ● Enable ○ Disable

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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

Related topics

Refer to the "SNMP" on page 191 for details.

SNMP v3 User field description

The following table describes the SNMP v3 user fields.

TABLE 39. SNMP V3 USER FIELD DESCRIPTION

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

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**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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

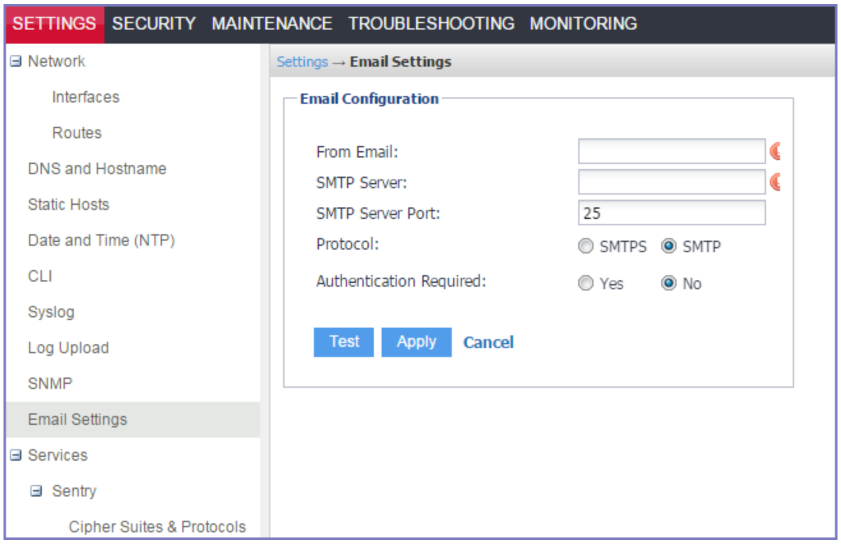
1. In the Standalone Sentry System Manager, navigate to **Settings > SNMP.**
2. Edit the default string.
3. Click **Apply**.

Email Settings

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. SMTP SETTINGS



From Email:
SMTP Server:
SMTP Server Port: 25
Protocol: ○ SMTPS ● SMTP
Authentication Required: ○ Yes ● No

Configuring the SMTP server information for Ivanti 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 SMPT, see "Field descriptions for SMTP settings" below.

Field descriptions for SMTP settings

The following table describes the fields for configuring SMTP settings.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 40. FIELD DESCRIPTIONS FOR SMTP SETTINGS

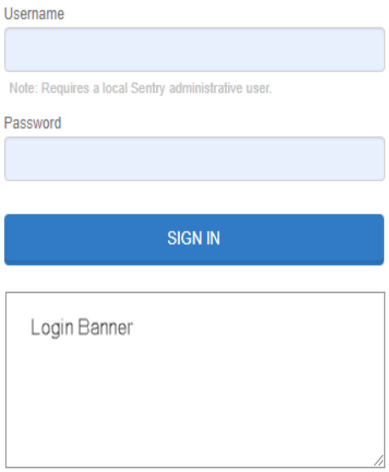
Field	Description
From Email	Specify the email address to use in the From field for all administrative email notifications.
SMTP Server	Specify the IP address or fully-qualified host name for the SMTP server the Ivanti Server will use.
SMTP Server Port	Specify the port configured for the SMTP server.
Protocol	If th 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.
Authentication Required	Specify whether this SMTP server requires authentication. In most cases, this field will be set to Yes.
User Name	If you select Yes for Authentication Required, then this field displays. Enter the user name required for SMTP authentication.
Password	If you select Yes for Authentication Required, then this field displays. Enter the password required for SMTP authentication.
Confirm Password	If you select Yes for Authentication Required, then this field displays. Confirm the password required for SMTP authentication.

Login

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

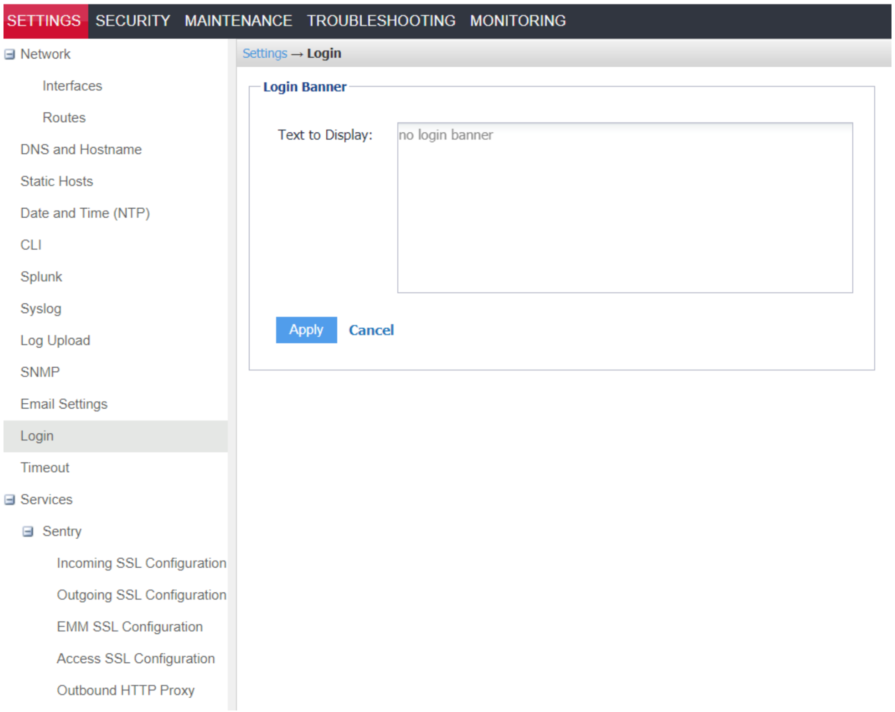
The banner does not appear on the Sentry log in page until the disclaimer is updated in the **Sentry Settings**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.



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.



Text to Display: no login banner

4. Click **Apply**.
5. Click **Yes** to confirm the configuration.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

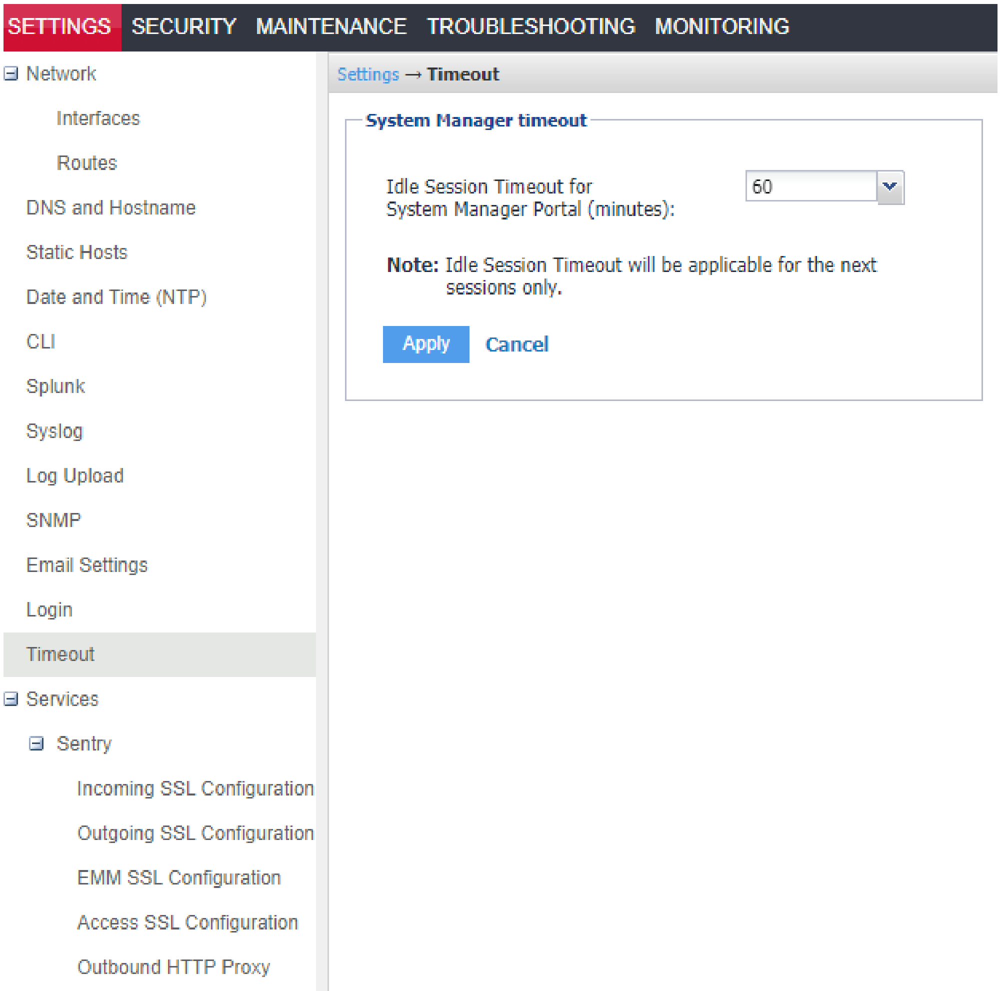
Timeout

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**.



System Manager timeout

Idle Session Timeout for System Manager Portal (minutes): 60

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

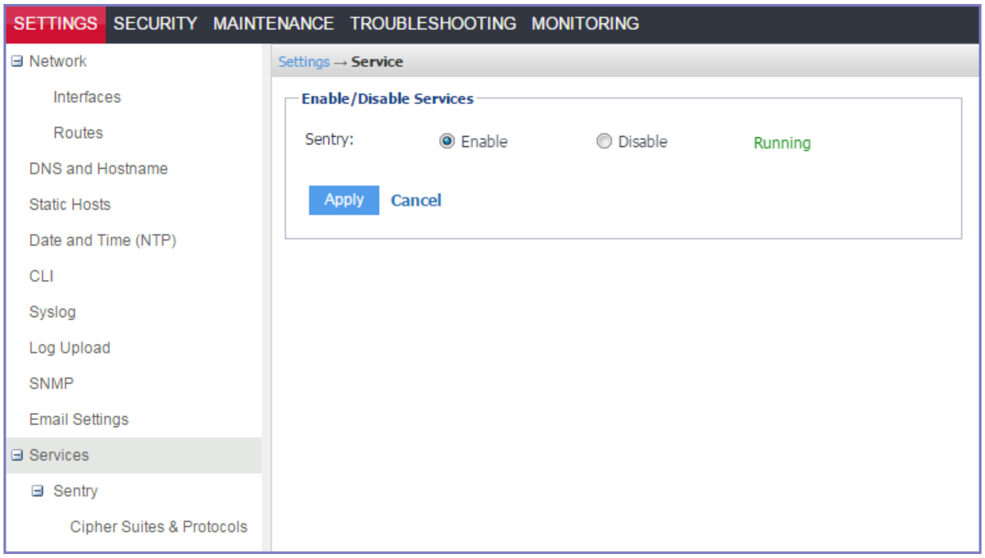
5. Click **Ok**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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



Settings → Service

Enable/Disable Services

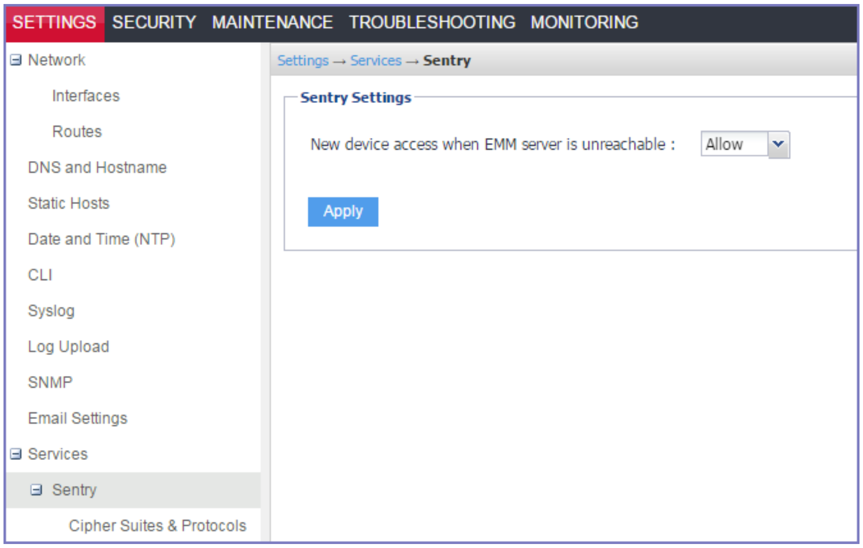
Sentry: ● Enable ○ Disable Running

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. NEW DEVICE ACCESS WHEN UEM IS UNREACHABLE



New device access when EMM server is unreachable : Allow

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 Ivanti Standalone Sentry cache, access to the ActiveSync server or backend resource if UEM is not reachable.

By default Ivanti Standalone Sentry allows new devices access to the server if the UEM is not reachable. In this case, for ActiveSync traffic, the ActiveSync server's policy is applied to the new device.

Changing the **New device access when UEM server is unreachable** setting does not restart Ivanti 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

Use the **Incoming SSL Configuration** page to configure ciphers and protocols for incoming traffic from device to Ivanti Standalone Sentry. You can do the following:

- View the **Available** and **Selected** protocols and cipher suites.
- Setup custom protocol and cipher suite configuration.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry includes a set of cipher suites and protocols. A default set of cipher suites and protocols are 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 Ivanti 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 Ivanti 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.

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.

The **Incoming SSL Configuration** page allows you to customize the default cipher suites and protocols settings to match the security and system needs of your enterprise. The custom configuration is preserved when you upgrade to the next version of Ivanti Standalone Sentry.

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 the Sentry 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

- TLSv1.2 (selected by default)
- TLSv1.1
- TLSv1
- SSLv2Hello

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- 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.

Customizing protocols and cipher suites configuration

You can customize which protocols and cipher suites are used with Ivanti Standalone Sentry.

Procedure

1. In Ivanti Standalone Sentry System Manager, go to **Settings > Services > Sentry > Incoming SSL Configuration**.

The **Use Default Cipher Suites and Protocols (recommended)** option is selected by default.

2. Select the **Use Custom Configuration** option.
3. Move protocols and cipher suites from the **Available** to **Selected** column or vice-versa as necessary.

The default cipher suites and protocols are colored blue.

4. Click **Apply** to apply 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

If you have customized the protocol and cipher configuration for Ivanti Standalone Sentry, you can switch back to the default configuration.

Procedure

1. In Ivanti Standalone Sentry System Manager, go to **Settings > Services > Sentry > Cipher Suites & Protocols**.
2. In the **Global Setting** section, select **Use Default Cipher Suites and Protocols (recommended)**.
3. Click **Apply** to apply the changes.

The cipher suites and protocols are reset to the default settings.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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.**

Outgoing SSL configuration

Use the **Outgoing SSL Configuration** page to configure ciphers and protocols for outgoing traffic from Ivanti Standalone Sentry to backend resources. You can do the following:

- **Enable Strict TLS** settings for Standalone Sentry SSL connections to backend resources.
- **Enable SNI**.
- View the **Available** and **Selected** protocols and cipher suites.
- Set up custom protocol and cipher suite configuration.

The default ciphers and protocols are colored blue.

Enable Strict TLS

You can enable strict TLS for outgoing traffic from Ivanti Standalone Sentry to backend resources. Strict TLS is not enabled by default. 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 Ivanti Standalone Sentry should use.

Server hostname verification with strict TLS

If strict TLS is enabled, Ivanti Standalone Sentry provides an additional layer of security by also verifying the server hostname. Server hostname verification is automatically enabled if **Enable Server TLS** is checked**.**

Impacts of server hostname verification

If the server’s hostname does not match the hostname in the server’s certificate, connection to the server will fail. The following connection error will be seen in Ivanti Standalone Sentry logs and in **System Manager > Monitoring**:

"Got exception during device-to-server processing, Sentry reporting error to client:server name mismatch, certificate issued to: [s01-trvlr-001]"

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Workaround: If there is a mismatch in the server hostname and hostname in the server's certificate, upload a new certificate that contains the correct hostname to the server, or disable strict TLS.

TLS settings for Ivanti Standalone Sentry in Ivanti EPMM

To enable strict TLS for outgoing traffic from Standalone Sentry, you should have also checked **Enable Server TLS** under **ActiveSync Configuration** or **TLS Enabled** under **AppTunnel Configuration.** These settings are configured in **Services > Sentry** in the Ivanti EPMM Admin Portal.

ⓘ If none of the service use TLS, the Outgoing SSL Configuration settings do not persist even if a change is made in the GUI.

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 Ivanti 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, Ivanti 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.

Cipher suites and protocols

Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti 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 Ivanti 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.

Making changes to the selected list of cipher suites may impact the performance and security of traffic through Ivanti 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.

Supported protocols

- TLSv1.2 (Selected by default)
- TLSv1.1
- TSLv1
- SSLv2Hello
- 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.

Enabling strict TLS

You can enable strict TLS and other trust settings for traffic from Ivanti Standalone Sentry to backend resources.

Procedure

1. In the Ivanti Standalone Sentry System Manager, go to **Settings > Services > Sentry > Outgoing SSL Configuration**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

2. In the **Strict TLS Settings** section, check **Enable Strict TLS**.

   Additional options are now available.

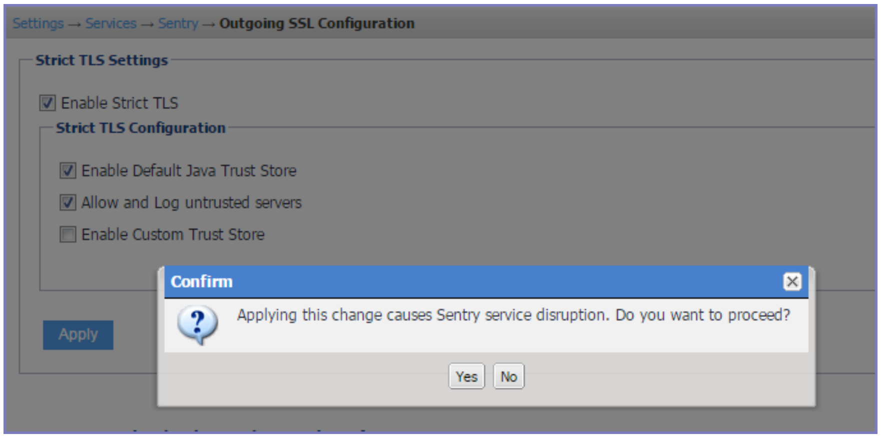
TABLE 41. ENABLE STRICT TLS OPTIONS

Item	Description
Enable Default Java Trust Store	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 the backend resource.
Allow and Log untrusted servers	Select to allow Ivanti Standalone Sentry to connect to a backend resource that does not use a trusted certificate in Java or custom trust store.
Enable Custom Trust Store	Select to upload certificates to the Ivanti Standalone Sentry trust store. Ivanti Standalone Sentry will use the certificates in the custom store to trust backend resources. Generally used if backend resources use self-signed certificates.

3. Click **Apply**.

   Confirm TLS setting change.

FIGURE 1. CONFIRM TLS SETTINGS CHANGE



Settings → Services → Sentry → Outgoing SSL Configuration

Strict TLS Settings

☑ Enable Strict TLS

Strict TLS Configuration

☑ Enable Default Java Trust Store

☑ Allow and Log untrusted servers

☐ Enable Custom Trust Store

Confirm

Applying this change causes Sentry service disruption. Do you want to proceed?

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. Click **Yes**.

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

5. Click **OK**.

Enabling Server Name Indication (SNI)

You can enable SNI for Standalone Sentry outgoing connections.

Procedure

1. In Ivanti Standalone Sentry System Manager, go to **Settings > Services > Sentry > Outgoing SSL Configuration.**

2. Click the **Enable SNI** check box.

3. Click **Apply**.

Creating a custom cipher configuration

You can customize the protocols and cipher suites the Ivanti Standalone Sentry will use.

Procedure

1. In Ivanti Standalone Sentry System Manager, go to **Settings > Services > Sentry > Outgoing SSL Configuration**.

   Ciphers and protocols are configured in the **Sentry to Backend Ciphers and Protocols Configuration** section.

   The **Use Default Cipher Suites and Protocols (recommended)** option is selected by default.

2. Select **Use Custom Configuration**.

3. Click on **Proceed** to continue.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 apply 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 Ivanti Standalone Sentry System Manager, go to **Settings > Services > Sentry > Outgoing SSL Configuration**.

2. In the **Sentry to Backend Ciphers and Protocols Configuration** section, select **Use Default Cipher Suites and Protocols (recommended)**.

3. Click **Apply** to apply 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.**

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 page 212.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- View the **Available** and **Selected** protocols and cipher suites. See "Cipher Suites and Protocols" on the next page.
- Set up custom protocol and cipher suite configuration. See "Cipher Suites and Protocols" on the next page.

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

When mutual authentication is enabled between Ivanti EPMM and Sentry, then that Sentry is enabled with Strict TLS Configuration.

Enabling Strict TLS

You can enable strict TLS for outgoing traffic from Ivanti Standalone Sentry to UEM. Strict TLS is not enabled by default for the UEM server. However, it is enabled for Ivanti Neurons for MDM. 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 Ivanti Standalone Sentry must use.

Procedure

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

Additional options are now available.

Item	Description
Enable Default Java Trust Store	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.
Allow and Log untrusted servers	Select to allow Ivanti Standalone Sentry to connect to UEM that does not use a trusted certificate in Java or custom trust store.
Enable Custom Trust Store	Select to upload certificates to the Ivanti Standalone Sentry trust store. Ivanti Standalone Sentry uses the certificates in the custom store to trust UEM. Generally used if UEM uses self-signed certificates.

3. Click **Apply**.
4. Click **Yes**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

The new TLS settings are applied and Ivanti Standalone Sentry restarts. It may take up to one minute for Ivanti 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 Ivanti Standalone Sentry for outgoing connections for the UEM server. However, SNI is enabled (read-only) for Ivanti Neurons for MDM 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 Ivanti Standalone Sentry System Manager, go to **Settings** > **Services** > **Sentry** > **EMM SSL Configuration**.
2. Click **Enable SNI**.
3. Click **Apply**.

Cipher Suites and Protocols

Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Making changes to the selected list of cipher suites may impact the performance and security of traffic through Ivanti 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.

The following protocols are supported:

- TLSv1.2 (Selected by default)
- TLSv1.1
- TSLv1
- SSLv2Hello
- 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 Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In Ivanti 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" below settings for Ivanti Standalone Sentry SSL connections to Access.
- "Server Name Indication (SNI)" on the next page.
- View the **Available** and **Selected** protocols and cipher suites. See "Cipher suites and protocols" on page 216.
- Set up custom protocol and cipher suite configuration. See "Customizing cipher suites and protocols" on page 216.

The **Access SSL Configuration page** allows the administrator the flexibility to configure Ivanti 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 Ivanti Standalone Sentry must use.

For more information on Strict TLS, see "Server hostname verification with strict TLS" on page 205, "Impacts of server hostname verification" on page 205 and "TLS settings for Ivanti Standalone Sentry in Ivanti EPMM" on page 206.

Procedure

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

1. In the Ivanti 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.

Item	Description
Enable Default Java Trust Store	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.
Allow and Log untrusted servers	Select to allow Standalone Sentry to connect to UEM that does not use a trusted certificate in Java or custom trust store.
Enable Custom Trust Store	Select to upload certificates to the Ivanti Standalone Sentry trust store. Standalone Sentry uses the certificates in the custom store to trust UEM. Generally used if UEM uses self-signed certificates.

3. Click **Apply**.
4. Click **Yes**.

The new TLS settings are applied and Standalone Sentry restarts. It may take up to one minute for Ivanti 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 Ivanti 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,Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Cipher suites and protocols

Ivanti 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 Ivanti 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 Ivanti 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.

Making changes to the selected list of cipher suites may impact the performance and security of traffic through Ivanti 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.

The following protocols are supported:

- TLSv1.2 (Selected by default)
- TLSv1.1
- TSLv1
- SSLv2Hello
- 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 Ivanti 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 Ivanti 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 Ivanti Neurons for MDM or Access.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Configuring Outbound HTTP Proxy

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

Procedure

1. In Ivanti Standalone Sentry System Manager, go to **Settings** > **Services** > **Sentry** > **Outbound HTTP Proxy.**
2. Select **Ivanti Neurons for MDM** to configure the outbound proxy server settings for Ivanti Neurons for MDM.

Enter the **Proxy Host**.

Enter the **Proxy Port**.

Enter the **User Name**.

Enter the **Password**.

3. Select **Access** to configure the outbound proxy server settings for Access.

Enter the **Proxy Host**.

Enter the **Proxy Port**.

Enter the **User Name**.

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 225

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

The following provide the format for audit log entries:

- "Audit log entry for a request" below
- "Audit log entry for a response" on the next page
- "Audit log entry for IP VPN response to tunnel establishment request" on page 221
- "Audit log entry for IP VPN internal connection" on page 222

Audit log entry for a request

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 42. FIELD DESCRIPTIONS FOR A REQUEST IN AUDIT LOG

Field	Description
publishTime	Actual time of log capture. Logging time might vary based on async strategies.
entryID	Unique for every audit entry. GUID.
useCaseID	ID of use-case to which this entry belongs to. This ID is used for relating Request/Response.
entryType	REQUEST.
userID	EMM User ID.
deviceID	Device identification.
deviceType	Type of device - iPhone, iPad etc.
serviceType	ActiveSync, CIFS, Access, APP_TUNNEL, TCP_TUNNEL, IP_TUNNEL.
serviceName	
clientHost	
clientPort	
requestUrl	URL used by device.
httpMethod	HTTP method used for this request.
applicationId	
forwardedFor	If proxy is forwarding request, this will have actual client host identifier.
contextHeaders	
serverHost	Details of downstream server.
serverPort	
action	ALLOW | BLOCK | NONE (Sentry compliance action taken - NONE - no compliance[Access])

Audit log entry for a response

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 43. FIELD DESCRIPTIONS FOR A RESPONSE IN AUDIT LOG

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

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 44. FIELD DESCRIPTIONS FOR IP VPN RESPONSE TO IVANTI TUNNEL ESTABLISHMENT REQUEST IN AUDIT LOG

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

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 45. FIELD DESCRIPTIONS FOR AN IP VPN INTERNAL CONNECTION ENTRY IN AUDIT LOGS

Field	Description
publishTime	
entryID	Unique for every audit entry. GUID.
useCaseID	ID of use-case to which this entry belongs to. This ID is used for relating Request/Response.
entryType	IP_VPN_CONN.
userID	
deviceID	
serviceType	IP_TUNNEL.
clientHost	
clientPort	
serverHost	
serverPort	
action	Compliance action like ALLOW, BLOCK, NONE.
type	Connection type: UDP or TCP.
sentryHost	Standalone Sentry hostname.
sentryPort	Standalone Sentry port.
sentryAddress	Standalone Sentry IP address.

Examples for audit log entries

Following are examples of audit log entries:

- "IPVPN audit log example" on the next page
    - "ActiveSync audit log example" on the next page
    - "HTTP tunnel audit log example" on the next page
    - "TCP tunnel audit log example" on page 225

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

IPVPN audit log example

```
2017 Nov  1 04:13:59 eapp123.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
43fbd6d7-258d-4d55-aa81-
cf1ba11533b4","entryType":"RESPONSE","userId":"hdhindsa","deviceId":"22002","serviceTy
pe":"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"}


2017 Nov  1 04:14:06 eapp123.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
43fbd6d7-258d-4d55-aa81-cf1ba11533b4","entryType":"IP_VPN_
CONN","userId":"hdhindsa","deviceId":"22002","serviceType":"IP_
TUNNEL","clientHost":"/24.5.120.210","clientPort":44258,"publishTime":"11/01/2017
4:14:06","entryId":"E-4190ad90-4391-47b1-b2b3-
298aec6aec5a","serverHost":"autodns001.auto.ivanti.com","serverPort":53,"action":"ALLO
W","type":"UDP"}


2017 Nov  1 04:14:06 eapp123.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
43fbd6d7-258d-4d55-aa81-cf1ba11533b4","entryType":"IP_VPN_
CONN","userId":"hdhindsa","deviceId":"22002","serviceType":"IP_
TUNNEL","clientHost":"/24.5.120.210","clientPort":44258,"publishTime":"11/01/2017
4:14:06","entryId":"E-b30097d0-f888-4437-b49d-
232d4f364815","serverHost":"216.58.192.10","serverPort":443,
"sentryHost":"10.10.57.239","sentryPort":446", "sentryAddress":"10.25.35.237",
"action":"ALLOW","type":"TCP"}
```

ActiveSync audit log example

```
2017 Nov  7 21:23:39 app101.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
ee3608c9-4c88-4b93-8221-
bd69cb4da900","entryType":"REQUEST","userId":"testuser0851","deviceId":"HroLBGueAofSIk
AcECcHMTTqd2","deviceType":"MD723LL","serviceType":"ACTIVE_
SYNC","serviceName":"ActiveSync","clientHost":"/10.11.80.93","clientPort":61693,"publi
shTime":"11/07/2017 21:23:38","entryId":"E-ee3608c9-4c88-4b93-8221-
bd69cb4da900","serverHost":"ex2013.auto19.ivanti.com","serverPort":443,"requestUrl":"/
Microsoft-Server-ActiveSync","httpMethod":"POST","action":"ALLOW"}


2017 Nov  7 21:23:41 app101.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
ee3608c9-4c88-4b93-8221-
bd69cb4da900","entryType":"RESPONSE","userId":"testuser0851","deviceId":"HroLBGueAofSI
kAcECcHMTTqd2","serviceType":"ACTIVE_
SYNC","clientHost":"/10.11.80.93","clientPort":61693,"publishTime":"11/07/2017
21:23:39","entryId":"E-49b382b2-07c9-4a82-87d3-
3f1f45751879","serverHost":"ex2013.auto19.ivanti.com","serverPort":443,"sentryHost":"1
0.10.57.239","sentryPort":446", "sentryAddress":"10.25.35.237", "httpStatus":"200"}
```

HTTP tunnel audit log example

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
2017 Nov  3 23:06:57 eapp074.auto.Ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
dd7086fc-9599-4581-a8bc-
5a9057ce085b","entryType":"REQUEST","userId":"testuser7331","deviceId":"62b6ae69-9ca8-
4176-85dd-11a7ecaee130","deviceType":"iPhone 6","serviceType":"APP_
TUNNEL","serviceName":"<ANY>","clientHost":"/10.11.205.8","clientPort":1821,"publishTi
me":"11/03/2017 23:06:57","entryId":"E-dd7086fc-9599-4581-
a8bc5a9057ce085b","serverHost":"wiki.ivanti.com","serverPort":443,"requestUrl":"https:
//wiki.ivanti.com/login.action?os_
destination=%2Findex.action&permissionViolation=true","httpMethod":"GET","applicationI
d":"com.ivanti.securebrowser","action":"ALLOW"}
```

```
2017 Nov  3 23:06:57 eapp074.auto.Ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
dd7086fc-9599-4581-a8bc-
5a9057ce085b","entryType":"RESPONSE","userId":"testuser7331","deviceId":"62b6ae69-
9ca8-4176-85dd-11a7ecaee130","serviceType":"APP_
TUNNEL","clientHost":"/10.11.205.8","clientPort":1821,"publishTime":"11/03/2017
23:06:57","entryId":"E-c0cd7a3d-1832-4b85-b28c-
7385d2b0eb0c","serverHost":"wiki.ivanti.com","serverPort":443,
"sentryHost":"10.10.57.239","sentryPort":446", "sentryAddress":"10.25.35.237",
"httpStatus":"200"}
```

TCP tunnel audit log example

```
2017 Nov  3 23:06:07 eapp074.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
bd77654c-42dc-48f3-9b2c-
9aa2d5d63650","entryType":"REQUEST","userId":"testuser7331","deviceId":"62b6ae69-9ca8-
4176-85dd-11a7ecaee130","serviceType":"TCP_TUNNEL","serviceName":"<TCP_
ANY>","clientHost":"/10.11.205.8","clientPort":1391,"publishTime":"11/03/2017
23:06:07","entryId":"E-bd77654c-42dc-48f3-9b2c-
9aa2d5d63650","serverHost":"googleads.g.doubleclick.net","serverPort":443,"application
Id":"com.google.chrome.ios","action":"ALLOW"}
```

```
2017 Nov  3 23:06:07 eapp074.auto.ivanti.com SENTRY_AUDIT:  INFO  {"usecaseId":"U-
bd77654c-42dc-48f3-9b2c-
9aa2d5d63650","entryType":"RESPONSE","userId":"testuser7331","deviceId":"62b6ae69-
9ca8-4176-85dd-11a7ecaee130","serviceType":"TCP_
TUNNEL","clientHost":"/10.11.205.8","clientPort":1391,"publishTime":"11/03/2017
23:06:07","entryId":"E-4fa74e1f-e0df-4093-9cd1-
a716aa0697ff","serverHost":"googleads.g.doubleclick.net","serverPort":443,
"sentryHost":"10.10.57.239","sentryPort":446", "sentryAddress":"10.25.35.237",
"httpStatus":"200"}
```

Health log representation and format

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

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

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

/var/log/mihealth_export/openPorts.log

sourcetype: sentry_mihealth_openPorts

```
Proto   Port
tcp     9090
...
udp    10012
```

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

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

/var/log/mihealth_export/hardware.log

sourcetype: sentry_mihealth_hardware

```
KEY                     VALUE
CPU_TYPE                Intel(R) Xeon(R) CPU E5504 @ 2.00GHz
CPU_CACHE               4096 KB
CPU_COUNT               1
HARD_DRIVES             sda (Virtual disk) 200 GB;
NIC_TYPE                <notAvailable>
NIC_COUNT               1
MEMORY_REAL             2054232 kB
MEMORY_SWAP             4128764 kB
```

/var/log/mihealth_export/cpu.log

sourcetype: sentry_mihealth_cpu

```
CPU    pctUser    pctNice  pctSystem  pctIowait    pctIdle
all       0.00       1.01       1.01       0.00      97.98
0         0.00       1.01       1.01       0.00      97.98
```

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

/var/log/mihealth_export/vmstat.log

/usr/bin/vmstat

sourcetype: sentry_mihealth_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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry Security Settings

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

Overview of Ivanti 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 46. CONFIGURATION LINKS IN THE SECURITY TAB

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

Local Users

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

- Command Line Interface (CLI)

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- System Manager access

Adding local users for System Manager

You can add local users in the Ivanti 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:

Field	Description
User ID	Enter the unique identifier to assign to this user.
First Name	Enter the user’s first name.
Last Name	Enter the user’s last name.
Password	Enter a password for the user. For password requirements, see "Password policy" on the next page
Confirm Password	Confirm the password for the user.
Group	This field is not configurable.
Email	Enter the user’s email address.
EDIPI	Enter the unique identifier assigned to this user. This is a mandatory field to configure CAC.

4. Click **Apply**.
5. Click **Save**.

Editing local users for System Manager

You can change the information for local users in the Ivanti 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.
   You cannot change the user ID.
4. Click **Apply**.
5. Click **Save**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Deleting local users for System Manager

You can delete local users in the Ivanti 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**.
   You cannot delete the user ID you logged in with.
4. Click **Save**.

Password policy

Password policy lets you configure complex passwords for Ivanti 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

1. On the Security tab, expand **Identity Source**.
2. Select **Password Policy**.
3. Configure the password policy for local users appropriately.

Policy	Values
Minimum Number of Character Classes in Password	1 to 4. Passwords must contain at least one upper case character, one lower case character, and one numeric character by default.
Lower Case	Enable or Disable
Upper Case	Enable or Disable
Numeric	Enable or Disable
Special Character	Enable or Disable. Password can contain special characters only from this set "!=({[_:-;~,)}]@#^|$".

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Policy	Values
Minimum Password Length	Passwords must have at least 6 characters. The length is set to 8 by default.
Maximum Password Length	Password length can extend up to 128 characters. The length is set to 32 by default.
Number of Failed Attempts	Failed password attempts are limited from 1 to 16. The number of attempts is set to 5 by default.
Auto-Lock Time	0-3600 seconds. You can set the time for password auto-lock.
Enforce Passcode History (Last 4 passwords)	Enable or Disable.

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 Ivanti 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 Ivanti 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).

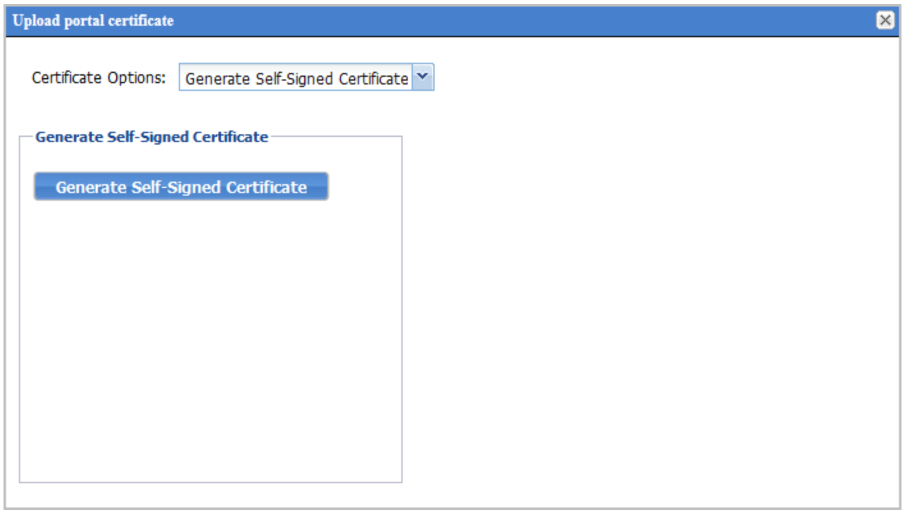
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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.

FIGURE 1. GENERATE SELF-SIGNED CERTIFICATE


Upload portal certificate
Generate Self-Signed Certificate
Generate Self-Signed Certificate

Certificate Options: Generate Self-Signed Certificate

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:

Field	Description
Common Name	Enter the server host name.
E-Mail	Enter the email address of the contact person in your organization who should receive the resulting certificate.
Company	Enter the name of the company requesting the certificate.

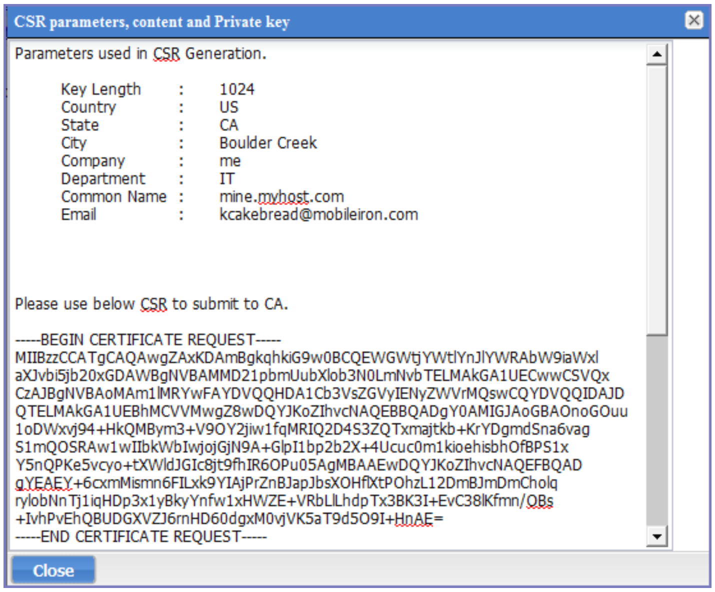
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Field	Description
Department	Enter the department requesting the certificate.
City	Enter the city in which the company is located.
State	Enter the state in which the company is located.
Country	Enter the two-character abbreviation for the country in which the company is located.
Key Length	Select 2048 or 3072 to specify the length of each key in the pair. Longer keys provide stronger security, but may impact performance.

4. Click **Generate**.

A message similar to the following displays.

FIGURE 2. CERTIFICATE REQUEST



```
Parameters used in CSR Generation.

        Key Length    :     1024
        Country       :     US
        State         :     CA
        City          :     Boulder Creek
        Company       :     me
        Department    :     IT
        Common Name   :     mine.myhost.com
        Email         :     kcakebread@mobileiron.com



Please use below CSR to submit to CA.

-----BEGIN CERTIFICATE REQUEST-----
MIIBzzCCATgCAQAwgZAxKDAmBgkqhkiG9w0BCQEWGWtjYWtlYnJlYWRAbW9iaWxl
aXJvbi5jb20xGDAWBgNVBAMMD21pbmUubXlob3N0LmNvbTELMAkGA1UECwwCSVQx
CzAJBgNVBAoMAm1lMRYwFAYDVQQHDA1Cb3VsZGVyIENyZWVrMQswCQYDVQQIDAJD
QTELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOnoGOuu
1oDWxvj94+HkQMBym3+V9OY2jiw1fqMRIQ2D4S3ZQTxmajtkb+KrYDgmdSna6vag
S1mQOSRAw1wIIbkWbIwjojGjN9A+GlpI1bp2b2X+4Ucuc0m1kioehisbhOfBPS1x
Y5nQPKe5vcyo+tXWldJGIc8jt9fhIR6OPu05AgMBAAEwDQYJKoZIhvcNAQEFBQAD
gYEAEY+6cxmMismn6FILxk9YIAjPrZnBJapJbsXOHflXtPOhzL12DmBJmDmCholq
rylobNnTj1iqHDp3x1yBkyYnfw1xHWZE+VRbLlLhdpTx3BK3I+EvC38lKfmn/OBs
+IvhPvEhQBUDGXVZJ6rnHD60dgxM0vjVK5aT9d5O9I+HnAE=
-----END 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 5 to the certifying authority.

Uploading certificates

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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:

Certificate	File to Select
Key file	The file created in "Generating a certificate signing request (CSR)" on page 233.
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.

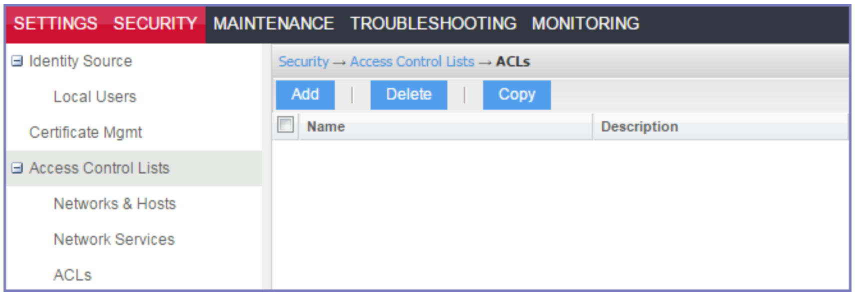
Viewing certificates

To view a certificate, in the Ivanti 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 Ivanti 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

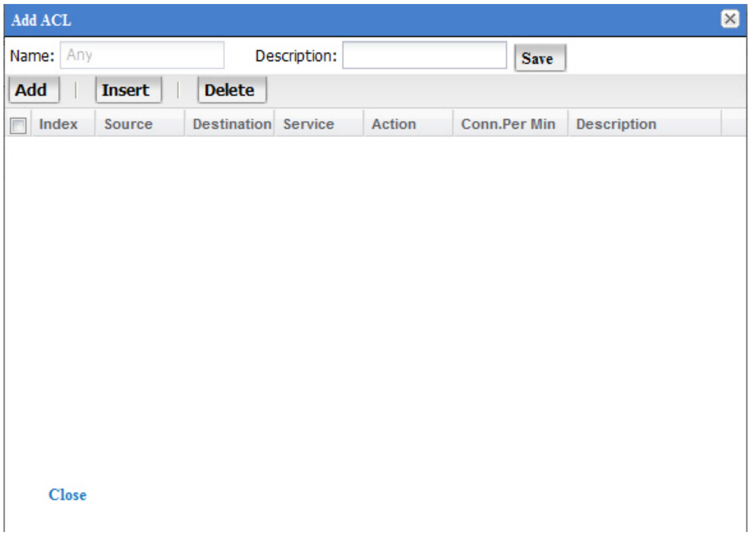
To configure an access control list in the Ivanti Standalone Sentry System Manager, go to **Security > Access Control Lists**.

Procedure

1. In the Ivanti 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:

Field	Description
Source Network	Select the network from which access will originate. This list is populated with the networks and hosts you created for use with ACLs. See “"Networks and Hosts" on page 238” on "Networks and Hosts" on page 238.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Field	Description
Destination Network	Select the network being accessed. This list is populated with the networks and hosts you created for use with ACLs. See “"Networks and Hosts" on the next page” on "Networks and Hosts" on the next page.
Service	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 “"Network Services" on page 239” on "Network Services" on page 239.
Action	Select Permit or Deny from the dropdown list.
Connections Per Minute	Enter the number of connections to allow per minute.
Description	Enter text to describe the purpose of this entry.

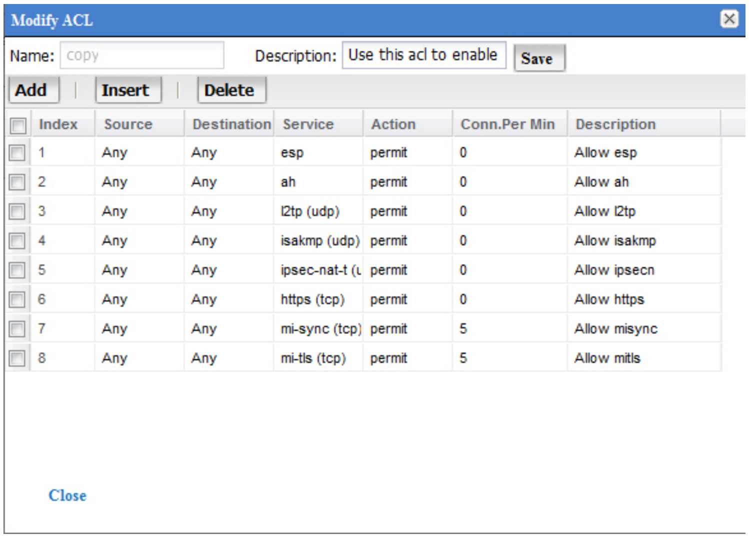
8. Click **Save**.

Editing an ACL

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

Procedure

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



Name: copy

Description: Use this acl to enable

Save

□	Index	Source	Destination	Service	Action	Conn.Per Min	Description
□	1	Any	Any	esp	permit	0	Allow esp
□	2	Any	Any	ah	permit	0	Allow ah
□	3	Any	Any	l2tp (udp)	permit	0	Allow l2tp
□	4	Any	Any	isakmp (udp)	permit	0	Allow isakmp
□	5	Any	Any	ipsec-nat-t (u	permit	0	Allow ipsecn
□	6	Any	Any	https (tcp)	permit	0	Allow https
□	7	Any	Any	mi-sync (tcp)	permit	5	Allow misync
□	8	Any	Any	mi-tls (tcp)	permit	5	Allow mitls

3. To delete an ACE, click its checkbox and click **Delete**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti Standalone Sentry, go to **Security** > **Access Control Lists**.

Procedure

1. In the Ivanti 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 Ivanti Standalone Sentry, go to **Security** > **Access Control Lists**.

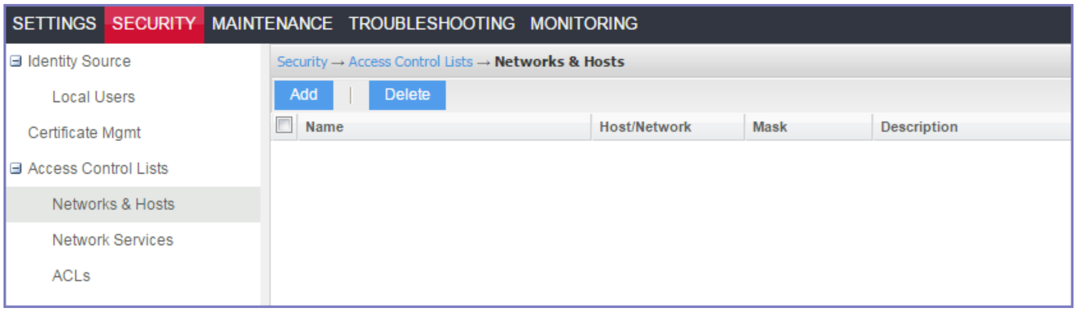
Procedure

1. In the Ivanti 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



Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

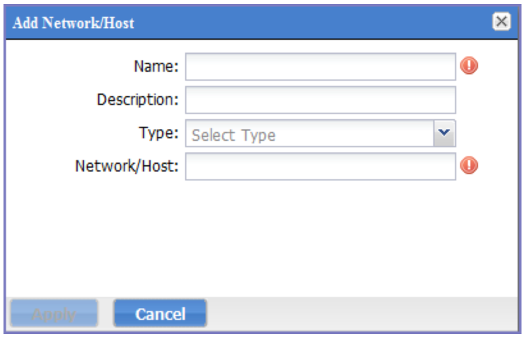
Adding a host or subnet for compiling ACLs

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

Procedure

1. Click **Add**.

FIGURE 2. ADD NETWORK HOSTS



2. Use the following guidelines for completing the displayed form:

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

3. Click **Save**.

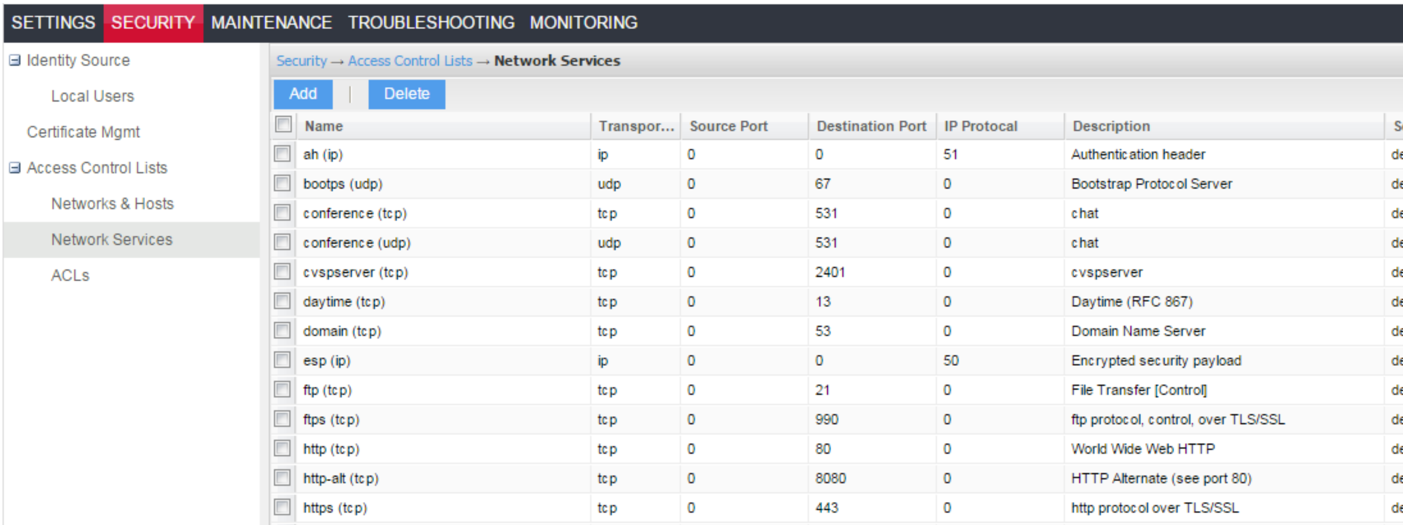
This host or network will now be available for ACLs configured in the ACLs screen.

Network Services

Use the Network Services screen to manage available services. Ivanti prepopulates this screen with common services.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. NETWORK SERVICES FOR ACL



□	Name	Transpor...	Source Port	Destination Port	IP Protocal	Description	S
□	ah (ip)	ip	0	0	51	Authentication header	de
□	bootps (udp)	udp	0	67	0	Bootstrap Protocol Server	de
□	conference (tcp)	tcp	0	531	0	chat	de
□	conference (udp)	udp	0	531	0	chat	de
□	cvspserver (tcp)	tcp	0	2401	0	cvspserver	de
□	daytime (tcp)	tcp	0	13	0	Daytime (RFC 867)	de
□	domain (tcp)	tcp	0	53	0	Domain Name Server	de
□	esp (ip)	ip	0	0	50	Encrypted security payload	de
□	ftp (tcp)	tcp	0	21	0	File Transfer [Control]	de
□	ftps (tcp)	tcp	0	990	0	ftp protocol, control, over TLS/SSL	de
□	http (tcp)	tcp	0	80	0	World Wide Web HTTP	de
□	http-alt (tcp)	tcp	0	8080	0	HTTP Alternate (see port 80)	de
□	https (tcp)	tcp	0	443	0	http protocol over TLS/SSL	de

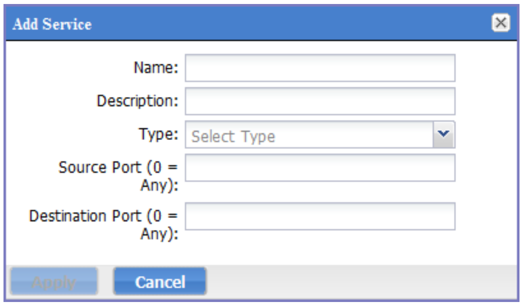
Adding a network service

To add a network service for compiling ACLs in the Ivanti 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:

Field	Description
Name	Enter a name to use to identify this service.
Description	Enter additional text provide supporting information about this service.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Field	Description
Type	Select TCP, UDP, or IP from the dropdown menu.
Source Port	Enter the number of the source port for this service. Enter 0 to allow any source port.
Destination Port	Enter the number of the destination port for this service. Enter 0 to allow any destination port.

3. Click **Save**.

Access Control Lists: ACLs

See “"Access Control Lists" on page 235” on "Access Control Lists" on page 235.

Advanced Sign-In Authentication

Use the settings in **Security** > **Advanced** to configure how administrators sign in to Ivanti Standalone Sentry System Manager. Administrators have the option to log in using password authentication or certificate authentication. Certificate authentication is done by enabling Personal Identity Verification (PIV) or Common Access Card (CAC). Password authentication is enabled by default.

To configure certificate authentication, in the Ivanti Standalone Sentry System Manager, got to **Security** > **Advanced** > **Sign-In Authentication**.

Sign-In Authentication

System Manager administrators are set up as local users in the System Manager in **Security** > **Local Users**. They can sign-in to the System Manager using one or both of the following methods:

- Password Authentication: A user name and password
  These are the credentials for the local users as set up in the System Manager in **Security** > **Local Users**. This authentication method is the default.

- Certificate Authentication: An identity certificate from a smart card
  Using an identity certificate from a smart card is supported only on desktop computers.

Certificate authentication is also supported in FIPS mode.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Certificates required for certificate authentication

A PEM formatted certificate is required for setting up certificate authentication to System Manager. You must upload the PEM certificate to the Standalone Sentry System Manager. Ensure that the PEM file contains the following:

- The issuing certificate authority (CA) certificate
- The supporting certificate chain
- The Intermediate CA

Ensure that the certificate is a valid certificate that has not expired or has not been revoked.

When users sign in to the Ivanti Standalone Sentry System Manager, they provide an identity certificate from a smart card. The System Manager authenticates the user’s identity certificate against the certificate that you uploaded.

For authentication of local users, set the User ID of the local user to the user identity from the identity certificate.

Certificate attribute mapping used in certificate authentication

When the Sentry local users present an identify certificate for authentication, Sentry authenticates the identity certificate against the issuing CA certificate or certificate chain you uploaded. As part of that authentication, Sentry makes sure the user identity in the identity certificate is a valid Sentry local user.

Therefore, when you upload the certificate used for authenticating Sentry local user's identity certificate, you should configure the Certificate Attribute Mapping section:

- which field from the identity certificate the authentication uses as the user identity. Your choice must match the Subject Alternative Name type you choose for generating the identity certificate. The choices are:
  - NT Principal Name
  - RFC 822 Name

  For the NT Principal Name, Sentry uses the User ID or Email Address in the Subject Alternative Name (SAN) in the identity certificate.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- The variable in Sentry System Manager to which the identity certificate field is mapped.
- Consider the case in which you specify the NT Principal Name as the field to use from the identity certificate, as the substitution variable to match. Sentry accepts both of the following formats as a match:
    - $USERID$
    - $EMAIL$
    - $EDIPI$ (for CAC only)
      Unique identifier for the user. EDIPI is a mandatory credential when configured for CAC. The value is set up in the System Manager in **Security** > **Local Users**. This value is for the Department of Defense only.
      However, If PIV is selected, then UserID and Email is mandatory configuration.

That is, the NT Principal Name and the substitution variable can have different formats, but match can be done as long as the domain and userid match.

Configuring certificate authentication to the System Manager

You can allow administrators to authenticate to the System Manager with the identity certificate on a smart card.

Before you begin
Have the PEM-formatted issuing CA certificate or certificate chain available to upload to Sentry.

Procedure

1. Log into **System Manager**.
2. Go to **Security** > **Advanced** > **Sign-In Authentication**.
3. Select **Certificate Authentication**.
4. Select PIV or CAC, depending on whether the identity certificate to authenticate is on a personal identity verification (PIV) card or common access card (CAC).

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

5. In **Select Certificate Attribute Mapping**:

   a. In the Map from attribute dropdown, select the user identity type in the identity certificate to use for authenticating the user.

   b. In the Map to attribute dropdown, select the variable with which to compare the user identity. If you selected CAC when choosing CAC versus PIV, you must select $EDIPI$.

6. Click **Upload Issuing CA Certificate** to open the **Upload Issuing CA Certificate** window.

7. Click **Choose File**, and select the PEM-formatted file that contains either the issuing CA certificate or the supporting certificate chain.

8. Click **Upload Certificate** > **OK**.

9. Click **Apply** > **OK**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Ivanti Standalone Sentry Maintenance Settings

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

Overview of Sentry maintenance features

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

TABLE 47. CONFIGURATION LINKS IN THE MAINTENANCE TAB

Setting	Description
Software Updates	Upgrade Standalone Sentry software.
Export Configuration	Save the system configuration file.
Import Configuration	Import a saved system configuration file.
Clear Configuration	Clear the current system settings.
Reboot	Restart the Standalone Sentry.

Updating Ivanti 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 309.

Before you begin
See the *Ivanti Standalone Sentry Release and Upgrade Notes* for release specific information.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Procedure

1. In Sentry System Manager, go to **Maintenance > Software Updates**.
2. **Software Version**: Check the Ivanti 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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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.

After you upgrade Ivanti Standalone Sentry, in the Ivanti EPMM Admin Portal, go to **Settings > Service Diagnostics**, and click **Verify** for the Ivanti Standalone Sentry. This action immediately updates the Standalone Sentry version in Ivanti EPMM. Otherwise, the Ivanti Standalone Sentry version in Ivanti EPMM is updated at the next sync.

Verifying that the upgrade is complete

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

Procedure

1. In Ivanti Standalone Sentry System Manager, go to **Maintenance** > **Software Updates**.

Confirm that the version displayed is the current version**.**

2. In Ivanti 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 48. SOFTWARE UPGRADE STATUS

Status	Description
Not Downloaded	The update is not yet downloaded. **Next Step:** Click **Download Now** or **Stage for Install** to download the update.
Download in progress	The download is in progress. Refresh the browser to update the status.
Downloaded	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.
Reboot to install	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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

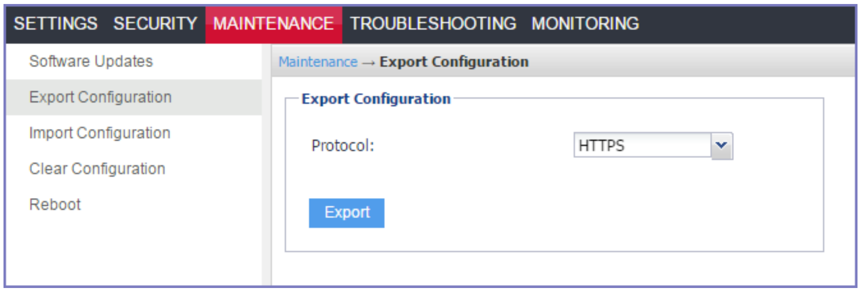
Exporting the configuration

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

Procedure

1. Select **Export Configuration**.

FIGURE 1. EXPORT CONFIGURATION



Protocol: HTTPS

2. Click **Export**.

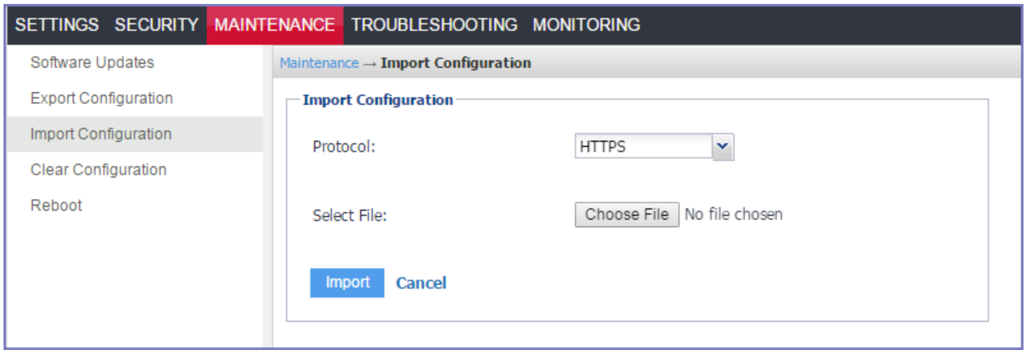
Importing a configuration

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

Procedure

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

FIGURE 1. IMPORT CONFIGURATION



Protocol: HTTPS

Select File: No file chosen

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

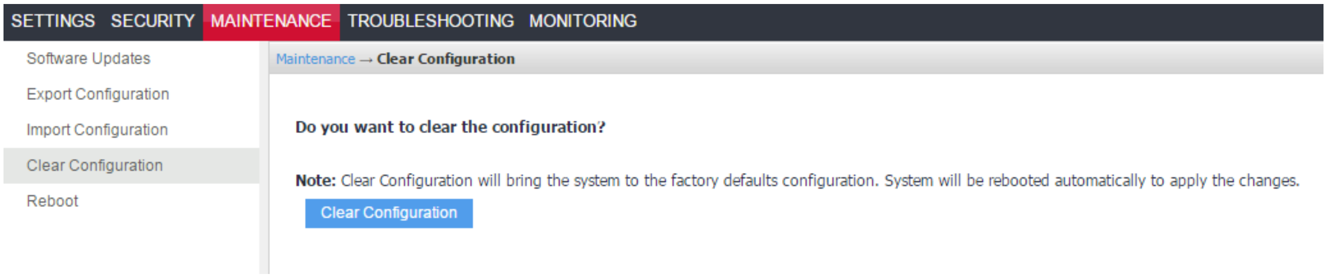
Clearing the configuration

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

Procedure

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

FIGURE 1. CLEAR CONFIGURATION



Do you want to clear the configuration?

Note: Clear Configuration will bring the system to the factory defaults configuration. System will be rebooted automatically to apply the changes.

3. Click the **Clear Configuration** button.

The appliance is automatically rebooted to apply the changes.

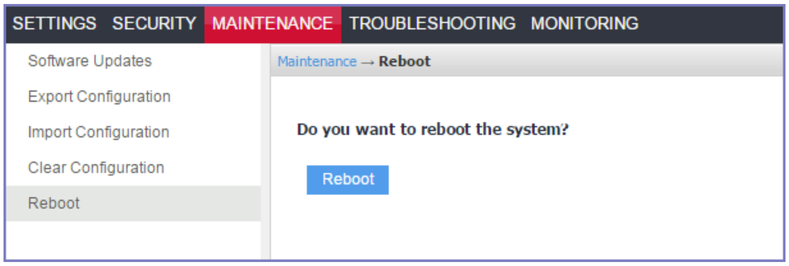
Rebooting

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

Procedure

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

FIGURE 1. REBOOTING



Do you want to reboot the system?

3. Click the **Reboot** button.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Troubleshooting

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

Overview of the Ivanti Standalone Sentry Troubleshooting tab

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

TABLE 49. CONFIGURATION LINKS IN THE TROUBLESHOOTING TAB

Settings	Description
Logs	Configure and upload log files.
Network Monitor	Produce a TCP dump for Sentry.
Service Diagnosis	Check the health of related servers.
Sentry Statistics	Produce an operational report.

Logs

The Logs page allows you to the following:

- Log management
- View module logs
- Export logs

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Log management

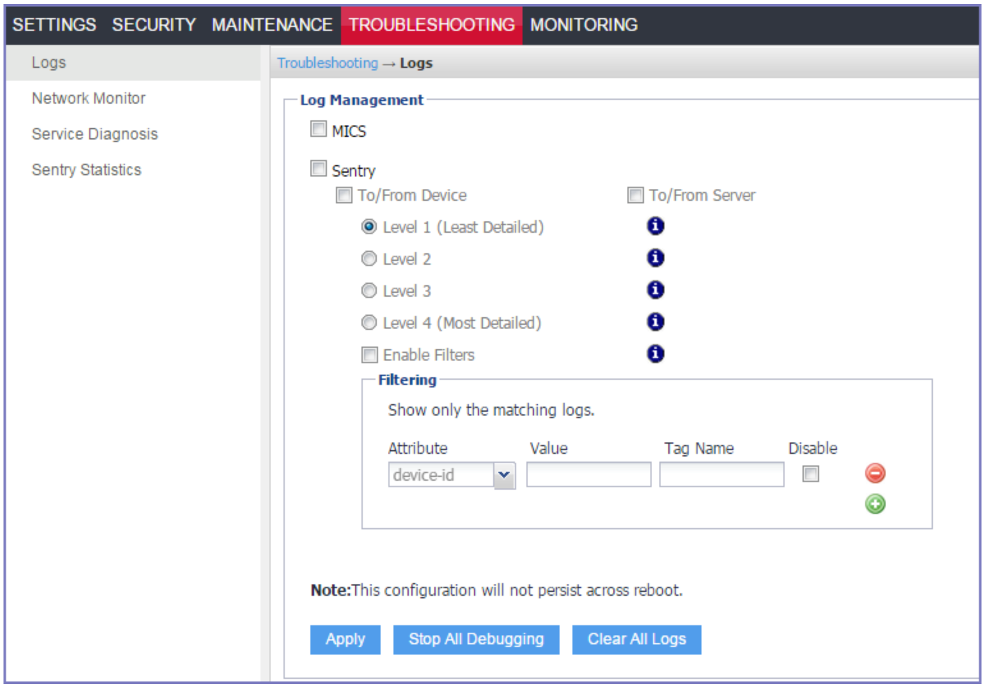
You can enable or disable logging and control the details collected in Sentry logs for the following services:

- 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



Log Management

□ MICS

□ Sentry

□ To/From Device □ To/From Server

● Level 1 (Least Detailed)

○ Level 2

○ Level 3

○ Level 4 (Most Detailed)

□ Enable Filters

Filtering

Show only the matching logs.

Attribute	Value	Tag Name	Disable
device-id			□

Note: This configuration will not persist across reboot.

The following table describes the options for managing logs.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 50. OPTIONS FOR MANAGING LOGS

Item	Description
MICS	Includes messages related to the MobileIron Configuration System module that supports the Sentry.
Sentry	Includes messages related to Sentry operation.
To/From Device	Includes messages related to interactions between Sentry and the registered ActiveSync devices.
To/From ActiveSync Server	Includes messages related to interactions between Sentry the configured ActiveSync servers.
Level 1	Includes HTTP response/request lines and a few supporting operational messages. This level of provides the least detailed logging.
Level 2	Includes Level 1 content, HTTP headers, and additional operational messages. Sufficient when network issues are suspected. Primarily used for troubleshooting AppTunnel issues.
Level 3	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 a 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.
Level 4	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

Related topics

- "Turning logging on or off" on the next page
  - "Filtering log entries" on the next page
  - "Disabling filters" on page 255
  - "Deleting filters" on page 255
  - "Viewing logs" on page 256

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Turning logging on or off

You can turn logging on or off by either selecting or deselecting 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

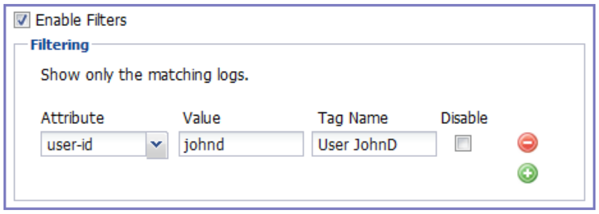
The Filtering section of the Log Management screen enables you to isolate entries based on the following attributes:

- 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



☑ Enable Filters

Filtering

Show only the matching logs.

Attribute	Value	Tag Name	Disable
user-id	johnd	User JohnD	□

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 51. DESCRIPTION OF AVAILABLE LOGS

Log Name	Description
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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

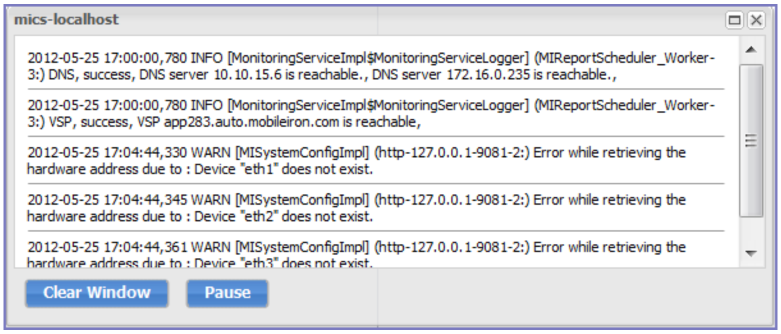
Viewing logs

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.

FIGURE 3. LOG VIEW



```
2012-05-25 17:00:00,780 INFO [MonitoringServiceImpl$MonitoringServiceLogger] (MIReportScheduler_Worker-
3:) DNS, success, DNS server 10.10.15.6 is reachable., DNS server 172.16.0.235 is reachable.,

2012-05-25 17:00:00,780 INFO [MonitoringServiceImpl$MonitoringServiceLogger] (MIReportScheduler_Worker-
3:) VSP, success, VSP app283.auto.mobileiron.com is reachable,

2012-05-25 17:04:44,330 WARN [MISystemConfigImpl] (http-127.0.0.1-9081-2:) Error while retrieving the
hardware address due to : Device "eth1" does not exist.

2012-05-25 17:04:44,345 WARN [MISystemConfigImpl] (http-127.0.0.1-9081-2:) Error while retrieving the
hardware address due to : Device "eth2" does not exist.

2012-05-25 17:04:44,361 WARN [MISystemConfigImpl] (http-127.0.0.1-9081-2:) Error while retrieving the
hardware address due to : Device "eth3" does not exist.
```

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.

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 or upload logs to the default support site or to an alternate site of your choosing.

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. If you have received a support ticket number associated with this upload, enter it in the **Support Ticket Number** field.
5. Click **Download**.

SFTP and HTTPS upload support for logs (Ivanti EPMM only)

You can upload logs directly to the default support site or an alternate site.

You can choose from the following log options:

- The Show Tech option provides important debug information for troubleshooting.
- The Show Tech (ALL) option provides additional exhaustive stats and logs.
- You can also select a specific Sentry module log from the dropdown list.

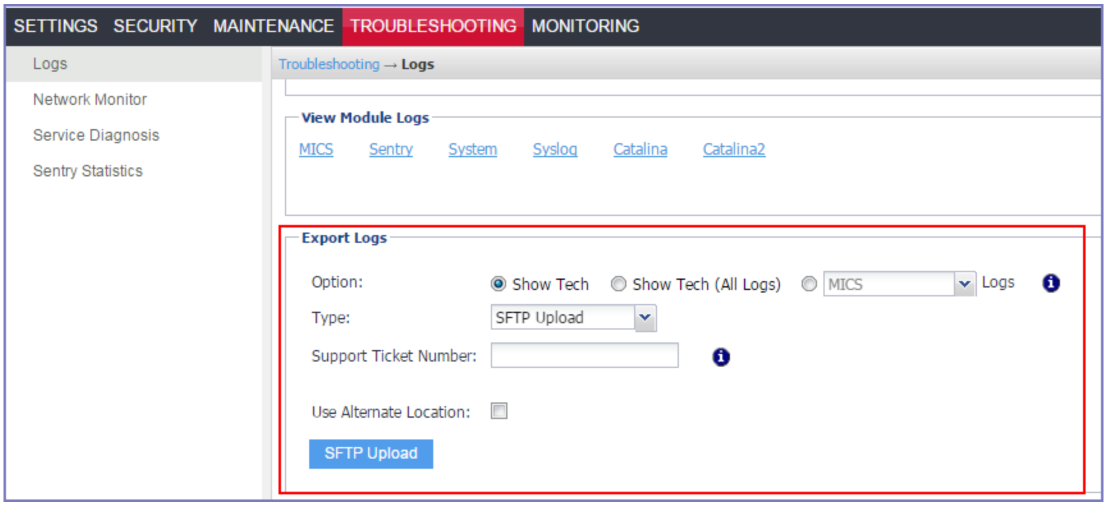
Uploading logs

The following procedure describes how to upload Sentry logs to the default support site or to an alternate site.

Procedure

1. Go to **Troubleshooting > Logs**.
2. Scroll down to the **Export Logs** section.

FIGURE 4. EXPORT LOGS



Option: ● Show Tech ○ Show Tech (All Logs) ○ MICS Logs

Type: SFTP Upload

Support Ticket Number:

Use Alternate Location: □

3. In the **Export Logs** section, select **SFTP Upload** or **HTTPS** Upload from the **Type** drop-down list, depending on the method of upload you want to use.

You must configure SFTP and/or HTTPS server authentication in the **Settings > Log Upload** so the log file can be received by your server.

By default, the output files are uploaded to the support site using the credentials configured in **Maintenance > Software Updates**.

4. If you have received a support ticket number associated with this upload, enter it in the **Support Ticket Number** field.
5. Select the **Use Alternate Location** check box and configure an alternate location. This location can be a backup location or the server of a support provider. This field is also used to upload information to a third party.

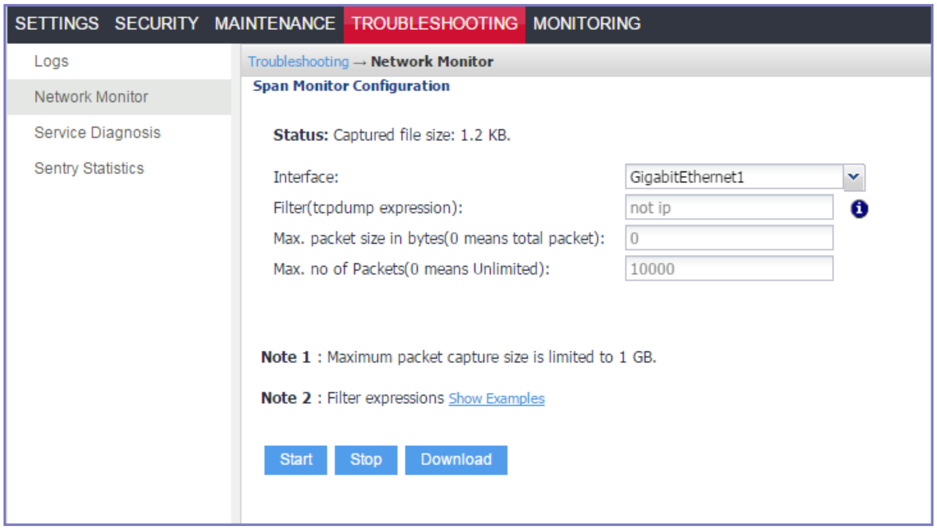
The following additional fields for the alternate location are displayed:

- **Host/IP** or URL
  For Host/IP, enter the server name. For example, support.mobileiron.com.
  For URL, enter the FQDN. For example, https://support.mobileiron.com
- **User Name**
- **Password**
- **Confirm Password**

6. Click **SFTP Upload** or **HTTPS Upload**.

Network Monitor

The **Network Monitor** page enables you to produce a TCP dump for an Ivanti Standalone Sentry physical interface. The information provided might assist in troubleshooting device connectivity problems. Click **Download** to store the results in a pcap file.



Span Monitor Configuration

Status: Captured file size: 1.2 KB.

Interface:	GigabitEthernet1
Filter(tcpdump expression):	not ip
Max. packet size in bytes(0 means total packet):	0
Max. no of Packets(0 means Unlimited):	10000

Note 1 : Maximum packet capture size is limited to 1 GB.

Note 2 : Filter expressions Show Examples

Use the following guidelines to complete this screen:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 52. NETWORK MONITOR FIELD DESCRIPTIONS

Option	Description
Interface	Select the physical interface for which you want to want to produce a TCP dump. If you have configured multiple interfaces, select **All** to get a TCP dump for all physical interfaces at one time.
Filter	not implemented.
Max. packet size	not implemented.
Max no. of Packets	not implemented.
Start	Click to start TCP dump. A growing file size indicates that the TCP dump is running.
Stop	Click to stop TCP dump. Click stop after reproducing the issue.
Download	Click to download TCP dump. If you click **Download** 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. A growing file size indicates that the TCP dump is running.

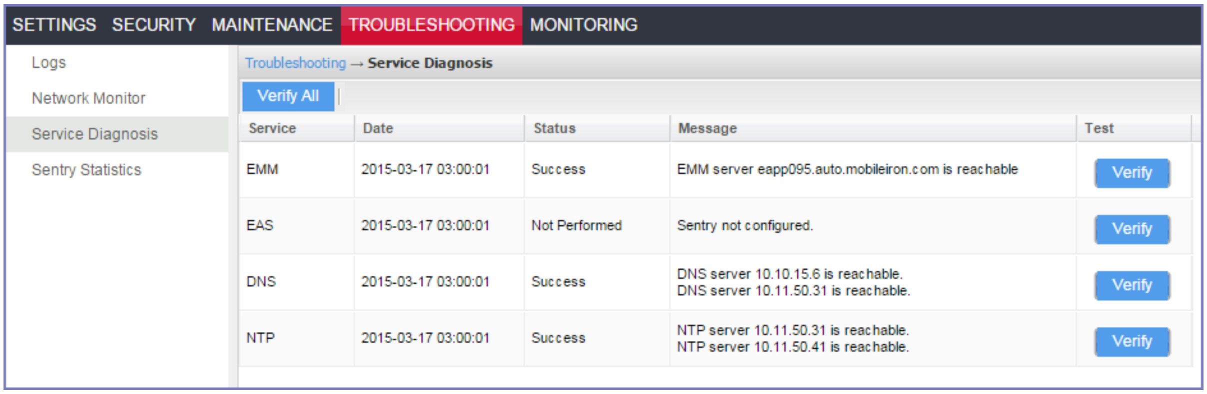
Service Diagnosis

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

- EAS
- NTP
- DNS
- UEM (Ivanti EPMM or Ivanti Neurons for MDM)

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

FIGURE 1. SERVICE DIAGNOSIS



Service	Date	Status	Message	Test
EMM	2015-03-17 03:00:01	Success	EMM server eapp095.auto.mobileiron.com is reachable	Verify
EAS	2015-03-17 03:00:01	Not Performed	Sentry not configured.	Verify
DNS	2015-03-17 03:00:01	Success	DNS server 10.10.15.6 is reachable. DNS server 10.11.50.31 is reachable.	Verify
NTP	2015-03-17 03:00:01	Success	NTP server 10.11.50.31 is reachable. NTP server 10.11.50.41 is reachable.	Verify

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** (Ivanti EPMM or Ivanti Neurons for MDM) entry causes Ivanti 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 Ivanti Standalone Sentry System Manager, go to **Troubleshooting > Service Diagnosis**.
- The Ivanti Standalone Sentry does not support the Ivanti EPMM version. In this case, although Ivanti EPMM is reachable, it is not compatible with the Ivanti Standalone Sentry.
- The Ivanti Standalone Sentry is not configured on any Ivanti EPMM.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 persists across Sentry restart. The settings in Sentry Statistics are saved as the following properties in /mi/alcor/config/v2/local/alcor-local.properties:

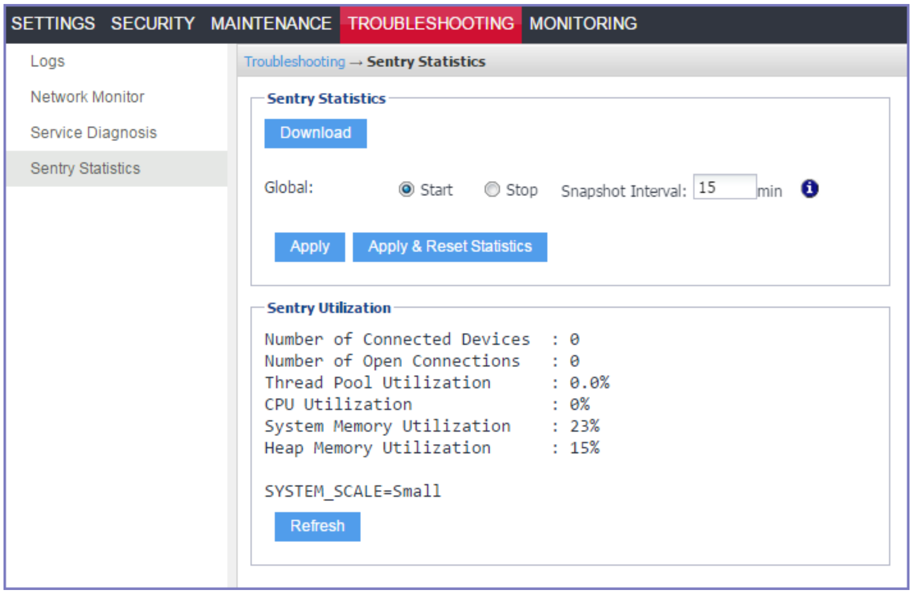
```
alcor.local.config.enable.sentry.global.statistics.report=true
alcor.local.config.statistics.log.interval.min=5
```

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

Use this page for the following:

- Downloading Sentry Statistics
- Viewing Sentry Utilization

FIGURE 1. SENTRY STATISTICS



Global: ● Start ○ Stop Snapshot Interval: 15 min

```
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%

SYSTEM_SCALE=Small
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 53. STATISTICS COLLECTION OPTIONS

Item	Description
Start	Select to start Sentry statistics collection. When the **Sentry Statistics** view shows **Start** as selected, statistics collection is written to global-stats.csv. This setting is not persistent. When Standalone Sentry restarts, the setting defaults to Stop. Statistics in global-stats.csv are archived
Stop	Select to turn off Sentry statistics collection. When the **Sentry Statistics** view shows **Stop** as selected, statistics collection is no longer written to global-stats.csv.
Apply & Reset Statistics	Click to clear the existing statistics file and restart statistics collection.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 **Appl**y.

ⓘ 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 Ivanti 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 54. SYSTEM UTILIZATION ALERT PARAMETERS

Parameter	Default Threshold
Thread Pool Utilization	80%
CPU Utilization	70%
System Memory Utilization	70%

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Monitoring

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

Overview of the Ivanti 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 55. STANDALONE SENTRY MONITORING

Alerts Viewer	View alerts
Alert Configuration	Configure notifications

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.

- 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 Ivanti Standalone Sentry is restarted, only the most recent 1000 lines will be displayed.

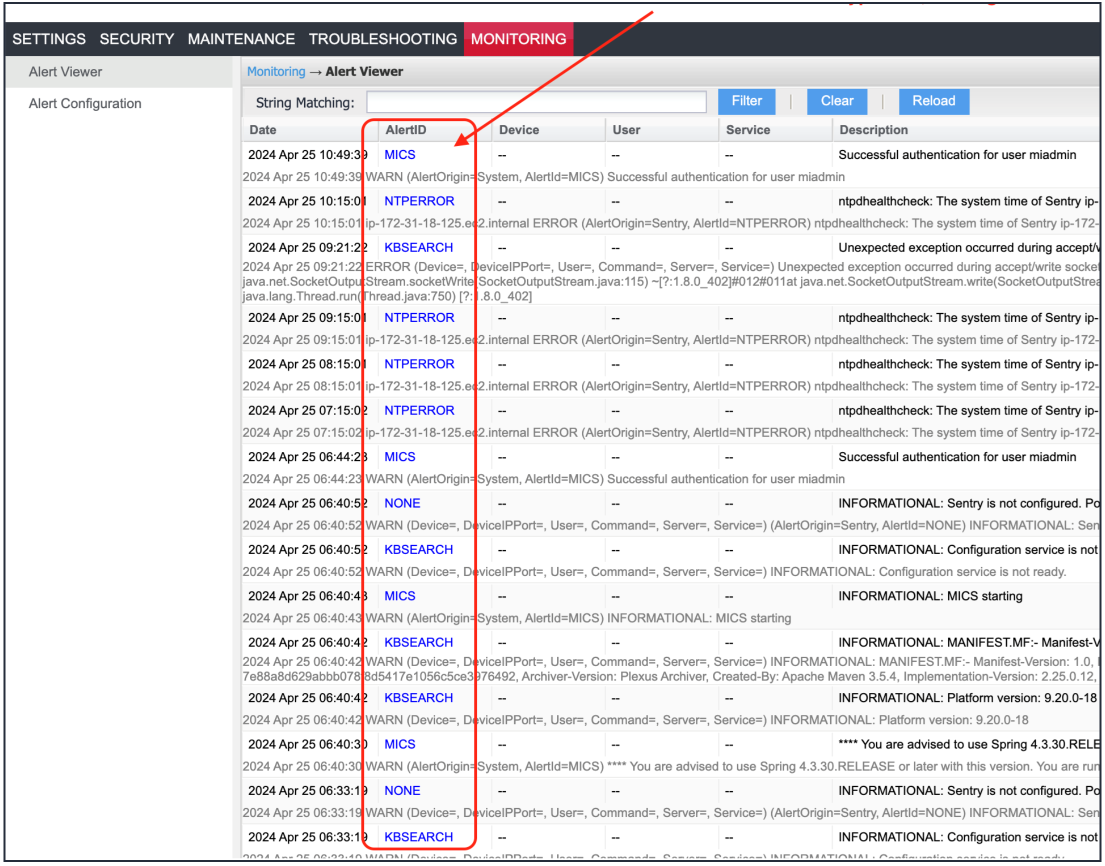
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Filtering Ivanti 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 Ivanti Standalone Sentry System Manager, go to **Monitoring > Alert Viewer**.



Date	AlertID	Device	User	Service	Description
2024 Apr 25 10:49:39	MICS	--	--	--	Successful authentication for user miadmin
2024 Apr 25 10:49:39 WARN (AlertOrigin=System, AlertId=MICS) Successful authentication for user miadmin					
2024 Apr 25 10:15:01	NTPERROR	--	--	--	ntpdhealthcheck: The system time of Sentry ip-
2024 Apr 25 10:15:01 ip-172-31-18-125.ec2.internal ERROR (AlertOrigin=Sentry, AlertId=NTPERROR) ntpdhealthcheck: The system time of Sentry ip-172-					
2024 Apr 25 09:21:22	KBSEARCH	--	--	--	Unexpected exception occurred during accept/w
2024 Apr 25 09:21:22 ERROR (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) Unexpected exception occurred during accept/write socket java.net.SocketOutputStream.socketWrite(SocketOutputStream.java:115) ~[?:1.8.0_402]#012#011at java.net.SocketOutputStream.write(SocketOutputStrea java.lang.Thread.run(Thread.java:750) [?:1.8.0_402]					
2024 Apr 25 09:15:01	NTPERROR	--	--	--	ntpdhealthcheck: The system time of Sentry ip-
2024 Apr 25 09:15:01 ip-172-31-18-125.ec2.internal ERROR (AlertOrigin=Sentry, AlertId=NTPERROR) ntpdhealthcheck: The system time of Sentry ip-172-					
2024 Apr 25 08:15:01	NTPERROR	--	--	--	ntpdhealthcheck: The system time of Sentry ip-
2024 Apr 25 08:15:01 ip-172-31-18-125.ec2.internal ERROR (AlertOrigin=Sentry, AlertId=NTPERROR) ntpdhealthcheck: The system time of Sentry ip-172-					
2024 Apr 25 07:15:02	NTPERROR	--	--	--	ntpdhealthcheck: The system time of Sentry ip-
2024 Apr 25 07:15:02 ip-172-31-18-125.ec2.internal ERROR (AlertOrigin=Sentry, AlertId=NTPERROR) ntpdhealthcheck: The system time of Sentry ip-172-					
2024 Apr 25 06:44:23	MICS	--	--	--	Successful authentication for user miadmin
2024 Apr 25 06:44:23 WARN (AlertOrigin=System, AlertId=MICS) Successful authentication for user miadmin					
2024 Apr 25 06:40:52	NONE	--	--	--	INFORMATIONAL: Sentry is not configured. Po
2024 Apr 25 06:40:52 WARN (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) (AlertOrigin=Sentry, AlertId=NONE) INFORMATIONAL: Sen					
2024 Apr 25 06:40:52	KBSEARCH	--	--	--	INFORMATIONAL: Configuration service is not
2024 Apr 25 06:40:52 WARN (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) INFORMATIONAL: Configuration service is not ready.					
2024 Apr 25 06:40:43	MICS	--	--	--	INFORMATIONAL: MICS starting
2024 Apr 25 06:40:43 WARN (AlertOrigin=System, AlertId=MICS) INFORMATIONAL: MICS starting					
2024 Apr 25 06:40:42	KBSEARCH	--	--	--	INFORMATIONAL: MANIFEST.MF:- Manifest-V
2024 Apr 25 06:40:42 WARN (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) INFORMATIONAL: MANIFEST.MF:- Manifest-Version: 1.0, 7e88a8d629abbb078 8d5417e1056c5ce3976492, Archiver-Version: Plexus Archiver, Created-By: Apache Maven 3.5.4, Implementation-Version: 2.25.0.12,					
2024 Apr 25 06:40:42	KBSEARCH	--	--	--	INFORMATIONAL: Platform version: 9.20.0-18
2024 Apr 25 06:40:42 WARN (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) INFORMATIONAL: Platform version: 9.20.0-18					
2024 Apr 25 06:40:30	MICS	--	--	--	**** You are advised to use Spring 4.3.30.RELE
2024 Apr 25 06:40:30 WARN (AlertOrigin=System, AlertId=MICS) **** You are advised to use Spring 4.3.30.RELEASE or later with this version. You are run					
2024 Apr 25 06:33:19	NONE	--	--	--	INFORMATIONAL: Sentry is not configured. Po
2024 Apr 25 06:33:19 WARN (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) (AlertOrigin=Sentry, AlertId=NONE) INFORMATIONAL: Sen					
2024 Apr 25 06:33:19	KBSEARCH	--	--	--	INFORMATIONAL: Configuration service is not
2024 Apr 25 06:33:19 WARN (Device=, DeviceIPPort=, User=, Command=, Server=, Service=) INFORMATIONAL: Configuration service is not ready.					

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.
   The following are the possible alerts:

   - MICS – Logout or Login should to MICS portal
   - RESTART – Restarting Sentry
   - KBSEARCH – Knowledgebase articles

4. Click **Clear** to clear the filter and return the complete set of alerts.

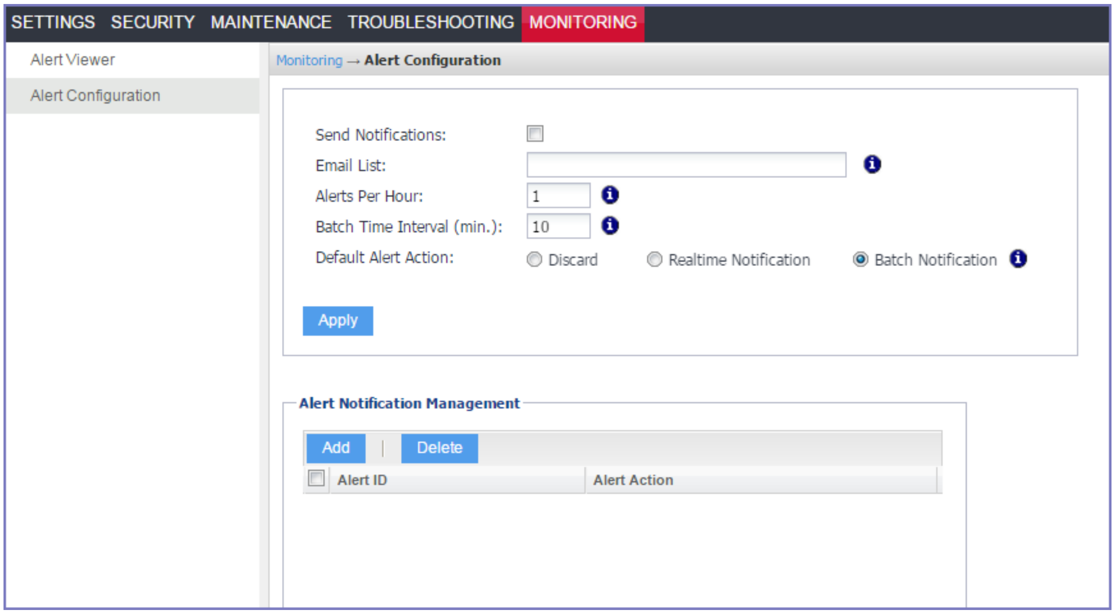
Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

5. 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 Ivanti Standalone Sentry alerts, such as email address to which notifications are sent.

FIGURE 1. ALERT CONFIGURATION



Send Notifications: □

Email List:

Alerts Per Hour: 1

Batch Time Interval (min.): 10

Default Alert Action: ○ Discard ○ Realtime Notification ● Batch Notification

□	Alert ID	Alert Action

Configuring Sentry alert notifications

Sentry alert notification is configured in the Ivanti 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.

Item	Description
Send Notifications	Select the checkbox to enable alert notifications.
Email List	Enter the email address to send the alerts. Enter multiple email addresses as a comma separated list.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Item	Description
Alerts Per Hour	Enter a number. This is the number of alerts in an hour that can be emailed to you. 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.
Batch Time Interval (min.)	Enter a number. Batch notifications are emailed at the interval set in this field.
Default	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. **Discard**: An email notification is not sent for the alerts. **Realtime Notification**: Email notification is sent immediately after the alert. Apply this action to alerts that require immediate attention. **Batch Notification**: Alerts are combined into a single email notification. Use batch notification for non-critical alerts.

3. Click **Apply.**

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

Managing alert notification

The alerts that contain the search text string were displayed on the Alert Viewer page. The **AlertID** column contains the alert ID. The administrator must configure the alert ID using **Add** in the Alert Notification Management. For more information, see "Alert Viewer" on page 265.

Configure a notification action to a Ivanti Standalone Sentry alert in **Monitoring** > **Alert Notifications** in the Ivanti 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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

4. Click **Apply**.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Command Line Interface

The Ivanti Standalone Sentry command line reference provides commands to configure many features that are also available in the Ivanti Standalone Sentry System Manager user interface. Many of the CLI commands are the same as the Ivanti EPMM CLI commands, but Ivanti Standalone Sentry does not support all of those commands.

For information on CLI commands common with Ivanti EPMM, see *Ivanti EPMM Command Line Interface (CLI) Reference*.

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

- Ivanti EPMM
- Ivanti Neurons for MDM

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 Ivanti Standalone Sentry:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 56. PURGING THE CACHE

Feature	Command
Purge the device cache	debug sentry device-cache purge all
Purge the device cache of a specific device	debug sentry device-cache purge entry <*device-id*> <*user-id*>
Purge the Kerberos cache	debug sentry kerberos-cache purge <*upn-string*>

- ***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
config#
```

- ***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&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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 57. LOGGING

Feature	Command
Enable Sentry logging	debug sentry log enable {device | server | both}
Specify filters	debug sentry log filter <*tag*> {device-id |device-ip | user-id | bundle-id | service-name | config-uuid} <*value*>
Specify verbosity	debug sentry log verbosity {level_1_lowest|level_2|level_3|level_4_highest}
Disable Sentry logging	no debug sentry log
Delete log filters	no debug sentry log filter <*tag*>
Disable initialization log messages	no debug sentry init-log
Enable initialization log messages	debug sentry init-log [level_1_lowest|level_2|level_3|level_4_highest]

- ***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:

```
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:

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
Successful
```

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

```
config# end
#show sentry log filter
                       TAG   ENABLED      TYPE              VALUE
                 KensDevice      true   user-id             ksmith
```

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

```
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:

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

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

```
no debug sentry log
```

Example of disabling the Sentry logging:

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

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

```
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 255. For information about disabling filters using the web interface, see "Disabling filters" on page 255.

Example of deleting filters using the CLI:

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

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- ***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 58. CONFIGURING GARBAGE COLLECTION

Feature	Command
Enable GC logging and rotation	sentry gc-log [*file-count*] [*file-size*] *file-count*: The number of GC log files to use when rotating logs. Enter a number between 1 and 100. The default is 5. *file-size*: 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.
Disable Sentry GC logging and rotation	no sentry gc-log Requires a restart of Sentry services for changes to take effect.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 59. MONITORING SENTRY

Feature	Command
Enable Sentry Monitor	debug sentry monitor enable
Disable Sentry Monitor	no debug sentry monitor enable
Port change for packet captures	debug sentry monitor capture port [*port_number*] If the port number is not provided, the default port 443 is used.
Duration of packet captures performed during data collection	debug sentry monitor capture time [*capture_time*] Capture time is measured in seconds. If *capture_time* is not provided, the default capture time of 600 seconds is used.
Sentry server is monitored for the number of running threads over the threshold	debug sentry monitor threads percentage [*percentage*] If the *percentage* is not provided, the default value for percentage is 90.
Sentry monitoring triggers a Sentry restart after the configured time.	debug sentry monitor trigger [*time_in_ minutes*] If the time is not set, the default time of 600 seconds is used.

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" on the next page
2. "Enabling log data" on page 280

To view Sentry facility configuration see:

- "Displaying syslog configuration" on page 281

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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]
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 60. ADDING A SYSLOG SERVER

Parameter	Description
server	IP address or hostname of the syslog server.
port	Syslog server port. Use port 514 if you are adding Monitor. If the port number is not provided, the default port 514 is used.
protocol	Protocol of the syslog server. The options are: • UDP • TCP

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 60. ADDING A SYSLOG SERVER (CONT.)

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

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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
sentry {audit | health-monitor}
```

TABLE 61. ENABLING LOG DATA

Feature	Command
Enable sentry audit log data	sentry audit
Enable sentry health monitoring	sentry health-monitor
Disable sentry audit	no sentry audit
Disable sentry health monitoring	no sentry health-monitor

Displaying syslog configuration

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

TABLE 62. DISPLAYING SYSLOG CONFIGURATION

Feature	Command
Display syslog configuration	show logging
Display sentry audit configuration	show sentry audit config
Display sentry health monitoring	show sentry health-monitor

Example

```
sentry# show logging

+-----------------------------+-------+----------+-----------------+-----------+------
--

 Hostname / IP Address        + Port  + Protocol + Facility Type   + Log Level + State

+-----------------------------+-------+----------+-----------------+-----------+------
--

 app1111.auto1.mycompany.com    514     UDP        health-monitor    info
enable
```

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- "Displaying Sentry configuration" below
- "Displaying information for entries in the device cache" below
- "Displaying information about Kerberos modules" on page 286
- "Displaying Sentry statistics" on page 287
- "Displaying information about servers" on page 291
- "Displaying Sentry system resources" on page 292
- "Displaying Sentry log configuration" on page 292
- "Displaying Sentry log filters" on page 293

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 63. DISPLAYING INFORMATION FOR ENTRIES IN THE DEVICE CACHE

Feature	Command
Display a list of entries in the Sentry device cache.	show sentry device-cache dump {all | active-sync | app-tunnel}
Display detailed information for a specific entry.	show sentry device-cache entry <*tunnel-id*> <*user-id*>
Display the entries associated with a device id	show sentry device-cache device <*device-id*>
Display the entries associated with a user id	show sentry device-cache user <*user-id*>
Display the entries with the specified number of minimum connections	show sentry device-cache min-connection <*value*>
Show the entries that need validation from UEM.	show sentry device-cache validation-pending {yes | no}
Show the status of the Sentry-device cache.	show sentry device-cache status
Show the connection status to UEM.	show sentry status

- ***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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- ***To display all entries associated with a specific device,*** type the following command:

```
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:

```
sentry# show sentry device-cache device 0V55EEVSRT5UVFA05AUBLF9O4S


S: Tunnel State {A:Allowed, B:Blocked, P:Policy Pending, W:Wipe Pending}

Vs: EMM Validation State {Y:validated, N:not-validated}

Cn: Connection count

Ver: AppTunnel Version or ActiveSync Version

Time: Timestamp of the last request or connection

Application[/ID]: Application[/ActiveSync Device ID (if application is 'ActiveSync')]

Tunnel-ID: Generic Tunnel ID


Index User           S Vs Cn Ver  Time                     Application[/ID]
           Tunnel-ID

1     testuser3351   A Y   0 14.1 2015-08-27 18:30:57 GMT
ActiveSync/0V55EEVSRT5UVFA05AUBLF9O4S 0v55eevsrt5uvfa05aublf9o4s


sentry#
```

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

```
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:

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


S: Tunnel State {A:Allowed, B:Blocked, P:Policy Pending, W:Wipe Pending}

Vs: EMM Validation State {Y:validated, N:not-validated}

Cn: Connection count

Ver: AppTunnel Version or ActiveSync Version

Time: Timestamp of the last request or connection

Application[/ID]: Application[/ActiveSync Device ID (if application is 'ActiveSync')]

Tunnel-ID: Generic Tunnel ID


Index User                            S Vs Cn Ver  Time
Application[/ID]               Tunnel-ID
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
1     testuser3351                     A Y   0 14.1 2015-08-27 18:30:57 GMT
ActiveSync/0V55EEVSRT5UVFA05AUBLF9O4S 0v55eevsrt5uvfa05aublf9o4s
sentry#
```

- ***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:

- ***To display information about the Standalone Sentry's connection to the UEM server ,*** enter the following command:

```
show sentry status
```

  Example of the command and its output:

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

Ivanti EPMM 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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
  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 64. DISPLAYING INFORMATION ABOUT KERBEROS MODULES

Feature	Command
Display the SPN, timeout, and cache size for Kerberos	show sentry kerberos
Display Kerberos UPN information	show sentry kerberos cache dump [*upn-filter*]
Display Kerberos information related to a specific UPN	show sentry kerberos cache upn <*upn-string*>

- ***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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- ***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 65. DISPLAYING SENTRY STATISTICS

Feature	Description
Display Sentry statistics for a specific device	show sentry statistics entry <*device-id*> <*user-id*>
Display Sentry global statistics for a specific device	show sentry statistics global [device|system] [*filter-string*]
Display complete global Sentry system statistics	show sentry statistics global system [*filter-string*]
Display complete global Sentry statistics for a server	show sentry statistics global server [*filter-string*]

- ***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 ApplDN6FM6SZDKPH testuser2885
 d-connection = 4
 s-connections = 4
 d-bytes-rcvd = 8572
 s-bytes-sent = 8368
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
 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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
 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
 attachments-encrypted = 0
 attachment-encrypt-failures = 0
 attachments-converted = 0
 attachments-replaced = 0
 attachment-replaced-failures = 0
 attachments-fwd-restored = 0
 attachments-fetched = 0
 attachments-embedded = 0
 attachments-renamed = 0
 attachments-size-MB = 0
 attachments-size-bytes = 0
 decryption-failures = 0
 d-http-503-s2c = 0
 d-http-503-c2s = 0
 d-http-400-c2s = 0
active-sync-status-reports = 0
sentry#
```

- ***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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
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
 peak-date-heap-mem-used-MB = Thu Aug 27 22:32:30 UTC 2015
 peak-buff-cached-mem-used-MB = 1189
 peak-date-buff-cached-mem-used-MB = Thu Aug 27 22:33:30 UTC 2015
 peak-process-virtual-mem-used-MB = 2988
 peak-date-process-virtual-mem-used-MB = Thu Aug 27 22:32:30 UTC 2015
 peak-process-resident-mem-used-MB = 1049
 peak-date-process-resident-mem-used-MB = Thu Aug 27 22:34:30 UTC 2015
 peak-cpu-% = 14
 peak-date-cpu-% = Thu Aug 27 22:32:30 UTC 2015
 peak-mem-% = 39
 peak-date-mem-% = Thu Aug 27 22:32:30 UTC 2015
 peak-running-threads = 1
 peak-date-running-threads = Thu Aug 27 22:33:21 UTC 2015
 peak-device-cache-size = 2
 peak-date-device-cache-size = Thu Aug 27 22:32:30 UTC 2015
 peak-user-url-cache-size = 0
 peak-date-user-url-cache-size = Thu Aug 27 22:32:30 UTC 2015
 peak-kerb-servtkt-cache-size = 0
 peak-date-kerb-servtkt-cache-size = Thu Aug 27 22:32:30 UTC 2015
sentry#
```

The full global statistics report can be downloaded in CSV format using the user interface. See "Sentry Statistics" on page 261.

- *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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
 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
Server                              Declared Last                 Failure
Name/IP                             Status   Failed               Count
--------------------------------------------------------------------------
                                    Live     Never                    0

Service Name : default
Service Type : Active-Sync
Server Scheduling : PRIORITY
Active Background Health Check : Enabled
Server                              Declared Last                 Last
 Failure
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
Name/IP                             Status   Successful          Failed
 Count
-------------------------------------------------------------------------------------
----------
ex2010sp3.enterprise.com      Live     08/27/2015 19:20:52  Never
0


Service Name : <TCP_ANY>
Service Type : App Tunnel
Server Scheduling : PRIORITY
Server                              Declared Last                 Failure
Name/IP                             Status   Failed               Count
--------------------------------------------------------------------------
                                    Live     Never                    0
sentry#
```

Displaying Sentry system resources

- *To display Sentry system resources*, type the following command:

```
show sentry utilization
```

Example:

```
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 273.

To display the Sentry log configuration, type the following command:

```
show sentry log
```

Example of a request to display log configuration information:

```
# show sentry log
    log-from-to = both
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
    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 273.

To display the Sentry log filters, type the following command:

```
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 276.

To display the Sentry GC configuration, type the following command:

```
show sentry gc-log
```

Debugging the in-memory and persistent device list

> ⓘ The CLI commands described in this section are available for Ivanti EPMM only.

CLI commands are available for debugging the persistent device list and the in-memory device list. You can access these commands from CONFIG mode.

Do not use these commands, which modify the list of devices on disk or in memory, unless Technical Support directs you to.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 66. DEBUGGING THE IN-MEMORY AND PERSISTENT DEVICE LIST

Feature	Command
Write the in-memory list of devices to disk.	debug sentry device-cache to-disk
Read the list of devices on disk into the in-memory list.	debug sentry device-cache from-disk
Update the in-memory list of devices based on Ivanti EPMM’s list of registered, allowed devices.	debug sentry device-cache from-Ivanti EPMM

- ***To write the in-memory list of devices to disk,*** enter the following command:

```
debug sentry device-cache to-disk
```

Example of a the command and its output:

```
#debug sentry device-cache to-disk
Wrote device-cache to disk. Number of devices written: 942
```

The number of devices written to disk is less than or equal to the number of devices in the in-memory device list. For example, devices for which the state (blocked, allowed) is unknown are not written to disk.

- ***To read the list of devices on disk into the in-memory list,*** enter the following command:

```
debug sentry device-cache from-disk
```

Example of a the command and its output:

```
#debug sentry device-cache from-disk
Restored device-cache from disk. Number of devices restored: 0
```

The number of devices restored to the in-memory device list is less than or equal to the number of devices in the persistent device list. For example, if a device in the persistent list is already in the in-memory list, it is not counted in this value.

- ***To update the list of devices in memory based on Ivanti EPMM’s list of registered, allowed devices,*** enter the following command:

```
debug sentry device-cache from-Ivanti EPMM
```

Example of a the command and its output:

```
#debug sentry device-cache from-Ivanti EPMM
Loaded and updated device-cache from Ivanti EPMM. Number of devices loaded:
7572
```

This command causes the Ivanti Standalone Sentry to get from Ivanti EPMM the list of registered devices that are allowed to access the ActiveSync server. This value is less than or equal to the number of devices in the in-memory device list. For example, the in-memory device list can also include unregistered devices and blocked devices.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Clearing the redirect URL

To clear a redirect URL from the Sentry, enter the following command:

TABLE 67. CLEARING THE REDIRECT URL

Feature	Command
Clear redirect URL	debug sentry device-cache clear-redirect-url {all | entry <*device-id*> <*user-id*>}

To clear the redirect URL for a specific device, enter the following CLI command:

```
debug 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
Appl7S032TF7A4S testuser2674
sentry/config#
```

To clear the redirect URL for all devices, enter the following CLI command:

```
debug 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 68. CONFIGURING ACCESS TO UEM

Feature	Command
Allow new devices to access the server.	sentry emm-fail-open
Block new devices from accessing the server.	no sentry emm-fail-open

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- *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 69. ENABLING AND DISABLING IPTABLES

Feature	Command
Enable the iptables service.	service iptables enable
Disable the iptables service.	no service iptables

- *To enable the iptables service*, type the following command in CONFIG mode:

```
service iptables enable
```

Example:

```
sentry/config# service iptables enable
sentry/config#
```

- *To disable the iptables service*, type the following command in CONFIG mode:

```
no service iptables
```

Example:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
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:

```
show service
 or
show running-config
```

Example:

```
sentry#show service
+------------+-----------+---------------
 Servicename + Enabled   + Max.Sessions
+------------+-----------+---------------
 ssh            yes        5
 ntp            yes
 iptables       yes
```

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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
ip name-server 10.10.15.6 0
ip name-server 10.11.50.31 1
ip domain-name auto.ivanti.com
ntp 172.16.0.235 1
hostname app264.auto.ivanti.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 70. CURL COMMANDS

Feature	Command
cURL to the ActiveSync destination server	curl active-sync <*dest*> [*port*] [*scheme*] [*protocol*] <*user*>
cURL to the AppTunnel destination server	curl app-tunnel <*dest*> [*port*] [method] [*scheme*] [*protocol*] [*user*]

- ***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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti Standalone Sentry self-signed certificate

You can regenerate the Ivanti 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 Ivanti 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. For iOS devices, click **View Certificate** for the Sentry entry in the Ivanti EPMM Admin Portal, under **Services > Sentry**. For AppConnect apps on Android devices, the AppConnect AppConfig must be re-pushed to the devices.

Regenerating the CA certificate, in addition, impacts Ivanti Tunnel. For Ivanti Tunnel, the CA certificate must be manually uploaded to the device. To manually push the Ivanti Standalone Sentry certificate to the device, follow the instructions in the *Using a Self-signed certificate with Standalone Sentry and Ivanti Tunnel* knowledge base article.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

How to regenerate the Ivanti Standalone Sentry self-signed certificate

To regenerate the Ivanti Standalone Sentry certificates, enter the following CLI command in configuration mode:

```
certificate {portal}
```

Table 71. Regenerating the Standalone Sentry self-signed certificate

Feature	Command
Regenerate Standalone Sentry self-signed portal certificate	certificate portal

To regenerate Ivanti 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:

```
debug sentry 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 `debug sentry 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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Checking connectivity to a KDC host

To check connectivity to a KDC host, enter the following CLI command in configuration mode:

```
debug sentry 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# debug sentry 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# debug sentry 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)
    at java.net.Socket.<init>(Socket.java:211)
    at com.ivanti.alcor.controller.SentryAdminController.debugKerberosKDC
(SentryAdminController.java:1085)
```

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 72. VERIFYING KERBEROS CONFIGURATION

Feature	Command
Request a kerberos ticket on behalf of a user with a host:port combination	debug sentry kerberos request-ticket host-port *<upn> <realm> <hostname> [port]* • *upn:* user's UPN • *realm:* user's REALM • *hostname*: backend server's hostname • *port:*: backend server's port The default value for port is 443.
Request a kerberos ticket on behalf of a user with an SPN	debug sentry kerberos request-ticket spn *<upn> <realm> <spn>* • *upn:* user's UPN • *realm:* user's REALM • *spn:* service principal name

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 Ivanti Standalone Sentry services

You can stop, start, or restart the following Ivanti Standalone Sentry services from the Ivanti Standalone Sentry command line interface (CLI):

- iptables
- tomcat
- tomcat2

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Restarting a service, stops the service and then restarts the service automatically.

TABLE 73. STOPPING AND RESTARTING STANDALONE SENTRY SERVICES

Feature	Command
Stop a service	service {iptables | tomcat | tomcat2} stop
Start a service	service {iptables | tomcat | tomcat2} start
Restart a service	service {iptables | tomcat | tomcat2} restart
View service status	service {iptables | tomcat | tomcat2} status

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 Ivanti Standalone Sentry services

- Stopping or restarting tomcat2 will impact access to Ivanti Standalone Sentry system manager UI and CLI commands. The Ivanti 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 Ivanti 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 Ivanti 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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
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 74. CONFIGURING KERNEL PARAMETERS

Feature	Command
Set this value to filter the kernel parameters.	kparam rp_filter [*kvalue*] *kvalue* is 0, 1 or 2.
Set this value to allow any unsigned integer value.	kparam log_martians [*kvalue*] *kvalue* is 0 or 1.
Set this value to allow safe recovery of any kernel malfunction.	kparam kernel_panic [*kvalue*] *kvalue* is an integer equal to or greater than 0.
Set this value to configure TCP SACK.	kparam tcp_sack [*kvalue*] *kvalue* is *kvalue* is 0 or 1.

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.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 75. SPLUNK FORWARDER SERVICE CLI COMMANDS IN STANDALONE SENTRY

Action	Command	Mode
Enable the Splunk forwarder service	service splunk-forwarder enable	CONFIG
Disable the Splunk forwarder service	no service splunk-forwarder	CONFIG
Start Splunk forwarder service	service splunk-forwarder start	EXEC PRIVILIGED
Stop Splunk forwarder service	service splunk-forwarder stop	EXEC PRIVILIGED
Status of the Splunk forwarder service	service splunk-forwarder status	EXEC PRIVILIGED
Restart the Splunk forwarder service	service splunk-forwarder restart	EXEC PRIVILIGED
Verify if the service is enabled or disabled	show service	EXEC

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. Ivanti recommends allowing HTTPS traffic on port 8443 from the corporate network, limited to Ivanti applications only. This service is intended for Ivanti Standalone Sentry System Manager and must have strictly controlled access. 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
distrupted.
Would you like to proceed? [y/n]: y
sentry/config# do show httpd protocol
+---------+---------------------------
  Port    +  TLS Protocols Enabled
+---------+---------------------------
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
  8443      TLSv1.1,TLSv1.2
  9090      TLSv1.1,TLSv1.2
sentry/config#
```

Checking TLS compliance

For improved security, Ivanti recommends that TLS v1.2 is used and TLS v1.0 and v1.1 are disabled. You can check which servers that Sentry connects with support TLS v 1.2 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 Ivanti Standalone Sentry is able to successfully connect with the server on TLS v1.2.

FAILED indicates that Ivanti 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 Ivanti 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 Ivanti Standalone Sentry connects with, enter the following command:

```
tlscheck all
```

To check TLS compliance for specified servers that Ivanti Standalone Sentry connects with, enter the following command:

```
tlscheck server server [port]
```

where:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- *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 Ivanti Standalone Sentry command line interface, enter the following command in EXEC PRIVILEGED mode:

```
#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 Ivanti Standalone Sentry. By default, HSTS is disabled.

Before enabling HSTS ensure the following:

- Ivanti 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.

Enabling SSL HSTS

To enable SSL HSTS, use the following CLI command in CONFIG mode:

```
httpd hsts enable [preload]
```

HSTS Preloading is not enabled by default and it can be enabled by setting the `preload` option to `yes`. The value of the preload is either `yes` or `no` and it is `no` by default.

If SSL HSTS is enabled, the following header is added to the HTTP response:

```
Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

If SSL HSTS is enabled with the preload option set to "yes", then the following header is added to the HTTP response:

```
 Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

Disabling SSL HSTS

To disable SSL HSTS, use the following CLI command in CONFIG mode:

```
no httpd hsts
```

After disabling HSTS, also clear HSTS for the Ivanti 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.

Viewing SSL HSTS

To view the current status of SSL HSTS, use the following CLI command in EXEC mode:

```
 show httpd hsts
```

For more information on HSTS, see https://tools.ietf.org/html/rfc6797

Enabling and disabling web service HSTS

Enabling HSTS (RFC 6797) enforces secure HTTPS connection between web services that talk to the web browsers and Ivanti Standalone Sentry. By default, HSTS is Enabled.

Restart Tomcat for enable/disable HSTS operations to take effect.

Before enabling HSTS ensure the following:

- Ivanti 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.

Use the CLI command line to run the following commands:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

- 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`

> ⓘ 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 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#
```

For more information on HSTS, see https://tools.ietf.org/html/rfc6797.

Upgrading using CLI

The following describe the steps for upgrading the Ivanti Standalone Sentry version using CLI:

1. "Configuring the update repo" on the next page
2. "Initiating the upgrade" on the next page
3. "Rebooting Ivanti Standalone Sentry" on page 311

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

4. "Verifying that the upgrade is complete" on the next page

Configuring the update repo

The following procedure describes the steps to update the repo.

Procedure

1. Log into the Ivanti 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.ivanti.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 *Ivanti Standalone Sentry Release Notes* for the release.

- 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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

Rebooting Ivanti Standalone Sentry

The following procedure describes the steps to reboot Ivanti 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 Ivanti Standalone Sentry 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 Ivanti Standalone Sentry and https://www.ivanti.com/support, 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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

TABLE 76. CONFIGURING PROXY SERVER FOR SOFTWARE UPGRADES

Feature	Command in CONFIG mode
Configure a proxy server for software upgrades	software outbound-proxy *<hostname> <port>* [*username*] [*password*] • *hostname :* The hostname or IP address of the proxy server. • *port:* Port number on the proxy server for Sentry. • *username*: Username to authenticate to the proxy server if authentication is required. • *password*: Password to authenticate to the proxy server if authentication is required.
Disable proxy server configuration	no software outbound-proxy
Feature	**Command in EXEC or PRIVILEGED mode**
Display proxy server information	show software outbound-proxy

Example for configuring a proxy server for software upgrades:

```
sentry/config# software outbound-proxy proxyserver.company.com 8080
```

Upgrading multiple Ivanti Standalone Sentry

You can upgrade multiple Ivanti 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 Ivanti 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 (Ivanti Neurons for MDM): Enter the IP Address for the Sentry on Ivanti Neurons for MDM that you want to upgrade.
- sentryUpgradeGroupList: Enter the Sentry groups that you want to upgrade.

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

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 Ivanti 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:

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.

```
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, Ivanti 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
```

Copyright © 2024, Ivanti, Inc. All Rights Reserved. Privacy and Legal.