EncrypTight Manager Release Note, v3.5

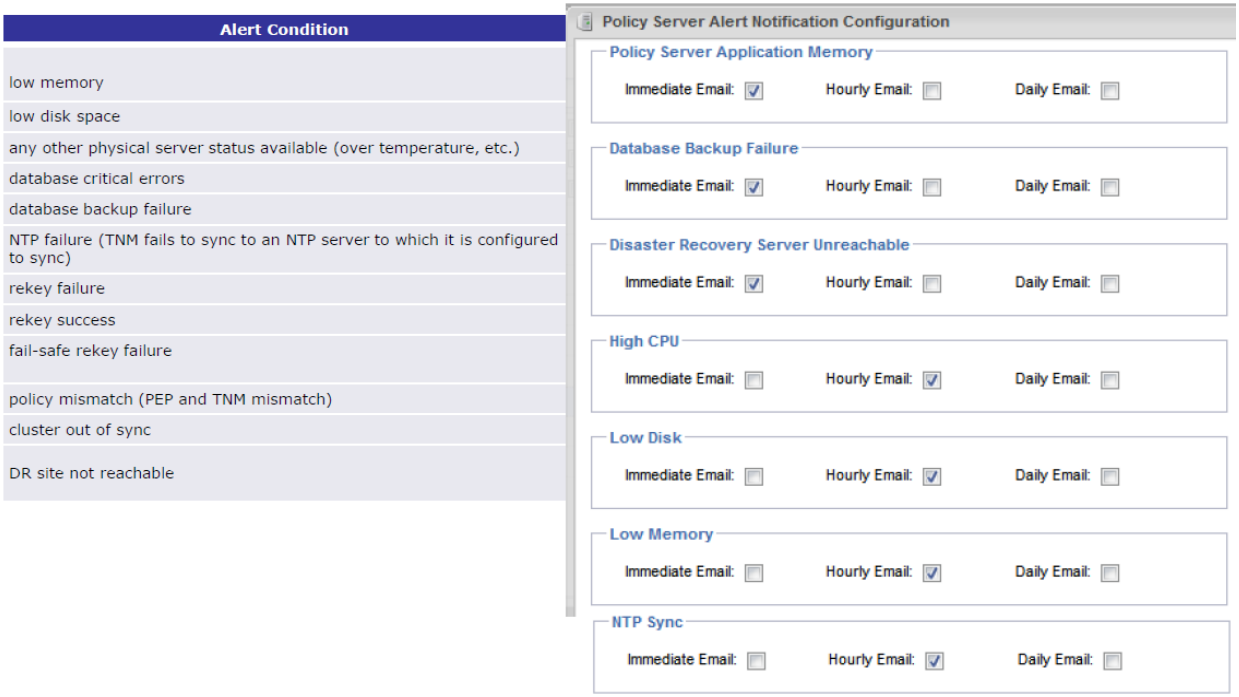
This release note describes new features, requirements, known issues, and bug fixes in EncrypTight Manager v3.5.

What's New in EncrypTight Manager v3.5

Alarms and email notifications

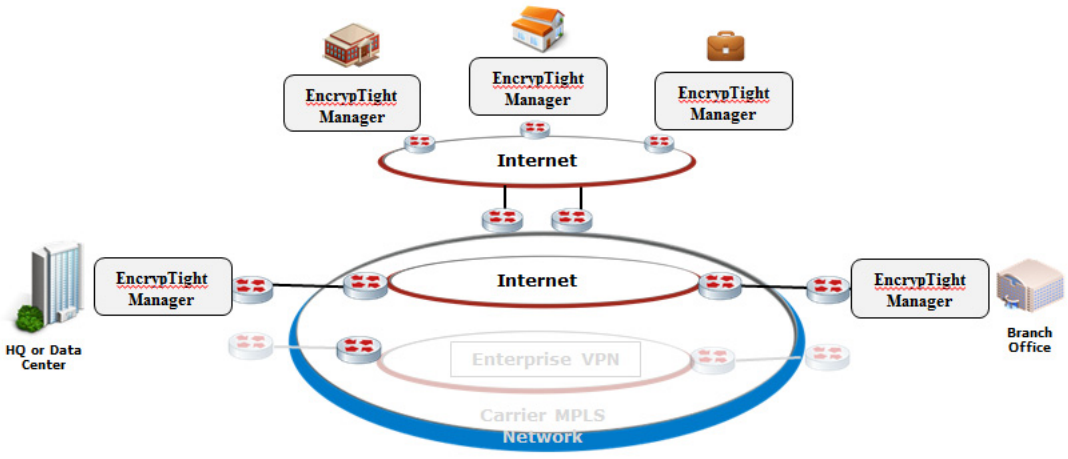
An email alert feature has been developed to notify the ETM users when there is problem with an ETEP or with ETM since we don't have separate network management system that collects traps and sends notifications.

- Alert reporting in ETM
- ETM sends email notifications on failure
  - ETEP alarms (Alert, Critical, Error, Warning, Notice) using syslog severity levels and which have equivalent ITU X.733 severity levels
  - Add support for ETM alerts and alert management within ETM
  - ETM email notification (immediate, hourly, daily)



Secure Mesh Internet

Figure 1 Secure Mesh Internet



Secure Mesh Internet Features

Secure full mesh encryption/authentication for all sites across the Internet

- Low latency - no need to hairpin traffic through a central site
- Better reliability than hub-and-spoke tunnels - all sites have direct connectivity to all other sites
- Works with business or consumer class Internet service (static or dynamic IP)

Central management for all sites

- Drag and drop provisioning for all sites
- No need to provision individual p-to-p tunnels
- Optional SaaS-based management – no need to deploy a server to manage it

Drop in solution

- Easy to deploy to existing networks without infrastructure changes
- Keep existing firewalls, gateways, and other edge security infrastructure

Regulatory compliance

- Powerful auditing and logging make it easy to demonstrate compliance with security mandates, such as PCI, HIPAA, and other PII legislation

Updated cryptographic algorithms.

- Added support for AES128_GCM and AES256_GCM as encryption algorithms for better performance.
- Algorithm name to be used in the CipherKey in TransformData aes-gcm and aes128-gcm
- A new optional attribute in TransformData "Salt" is also added. With GCM,we need to ensure unique IVs between rekeys for data security. ETM is already passing down a salt guaranteed to be unique per PEP, we just need to use this in the control plane and dataplane to generate the IV.

NOTE

AES-GCM is not fully supported at this time, and is available for BETA trails only.

TACACS+ AAA

In small network environment anybody can log-in into the network devices to make configuration changes.For these devices to provide network access protection, username and password are stored locally on device.

The main disadvantage of above localized credential is there is that, there is a minimum or no control of such credential integrity. For example, someone could log in and make changes to the the password with out others knowledge, This change will not allow others to log in anymore without knowing the new password.

The best practice is to have more control through centralized AAA (Authentication, Authorization, Accounting) server. This server is the sole location for storing the user credentials.

The AAA server can also perform accounting of all the operations.

TACACS+ (Terminal Access Controller Access-Control System Plus) is a remote authentication protocol that is used to communicate with an AAA server.

TACACS+ allows a remote host to communicate with an authentication server in order to determine if the user has any access to the network device.

TACACS+ support is added for ETM and all the ETEP platforms ET0005A, ET0010A/ET0100A/ ET1000A, ET10000A, ETVEP, for ETEP release 2.3 and ETM release 3.5.

Figure 2 TACACS Topology #1

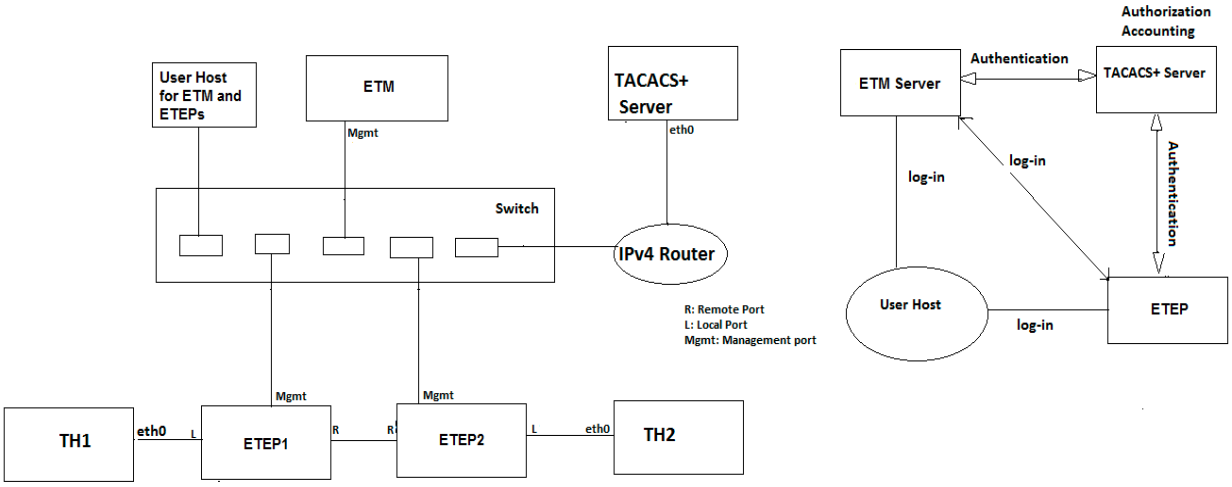
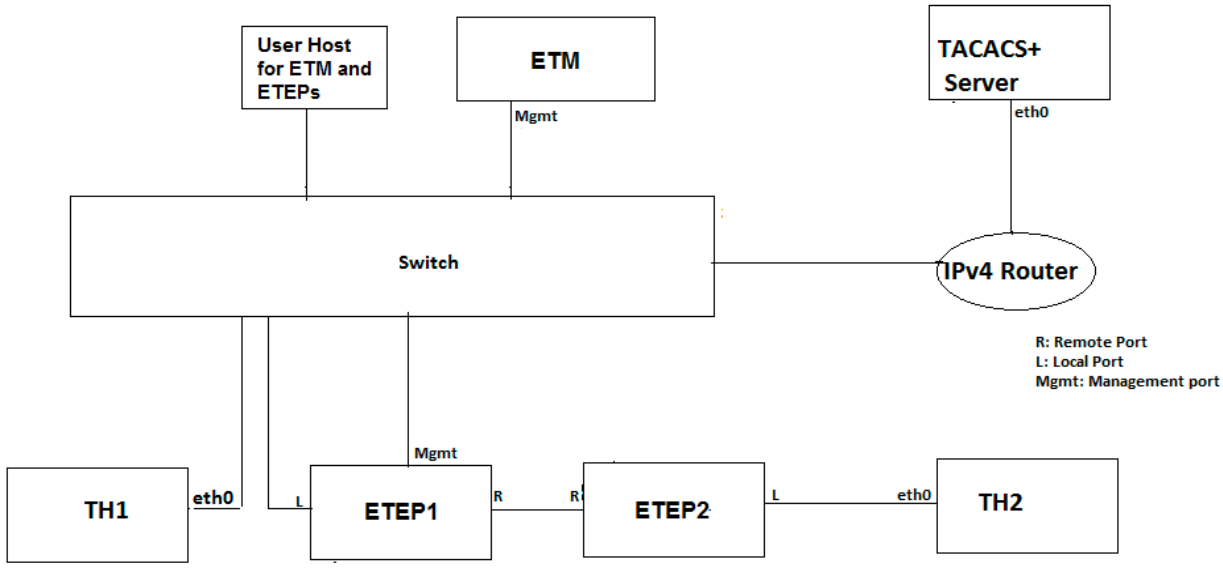


Figure 3 TACACS Topology #2



Safe Mode

Safe Mode allows the PEP to be managed and recovered when unexpected failures occur.

Allows PEP to be reachable even under failure conditions.

- Software defect
- Unreadable configuration
- Configuration error

Safe Mode Recovery

PEP goes into safe mode when it detects a failure (e.g. can't load the present or previous policy or configuration)

When going into safe mode:

- PEP sends an alert when entering safe mode
- Load a policy to pass traffic – two supported policy modes (cfg. via ETM):
  - In "All traffic" mode, the PEP loads a policy rule to pass all traffic in the clear
    - This provides the best chance for recovery while the network continues to pass traffic
    - May require the administrator to push a temporary clear rule for other PEPs
  - In "Management traffic" mode, the PEP loads a policy rule to drop all traffic except management traffic – no user traffic is passed in this mode
    - Favors security over availability – no plaintext traffic is allowed to pass (only mgmt. traffic)

To get out of safe mode, admin:

- Provisions new policy and new configuration, and then restart the PEP
- Clears the PEP alarm

"Not Encrypting" alarm

Provide an alert if network traffic is not encrypted

Details:

- Immediate alert whenever a ETEP is not encrypting
- User specifies how much traffic should be encrypted, and the alarm is generated if the fraction of encrypted traffic falls below the threshold (T1). Alarm clears when the fraction of encrypted traffic goes above a threshold (T2).
- Audit log entries generated for creating and clearing the "Not Encrypting" alert.

Two-factor authentication

- Require the user to use a second factor to authenticate to ETM
- The two factors are: "Something you know" and "Something you have"
- The second factor is typically a smartphone that generates a one-time password
- Details:
  - Two use cases:
  - 1. If the user has a device that can generate a one time password (OTP), he enters his username into ETM, and enters a PIN into his device, and the device generates an OTP and the user enters the OTP as his password into ETM. For the OTP first use case, the user enters their password, and then appends a forward slash '/' and then the one-time password (OTP) generated by their device to log in (i.e., password/OTP).

- 2. If the user does not have a device that can generate a OTP, he enters his username and ETM password into ETM, and if ETM accepts the username/password, then ETM emails the user a OTP. The user then enters his username and the OTP from the email to log in
- The platform administrator can unlock a tenant by entering only the ETM password
- Based on open source Mobile-OTP implementation

Figure 4 ETM Server Configuration for OTP

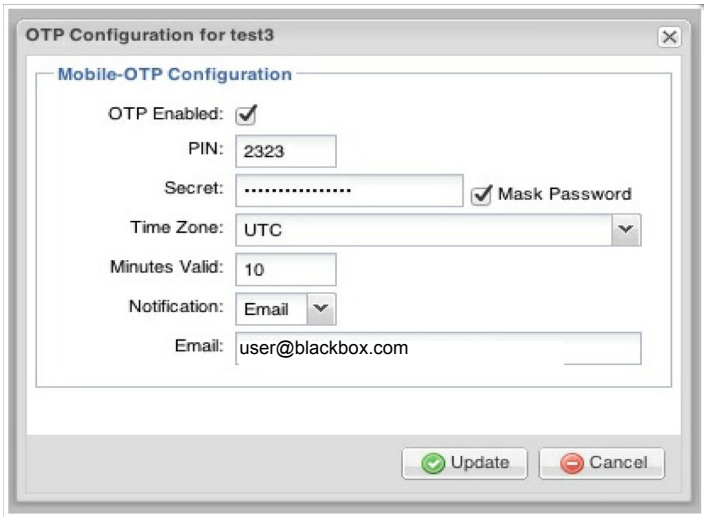
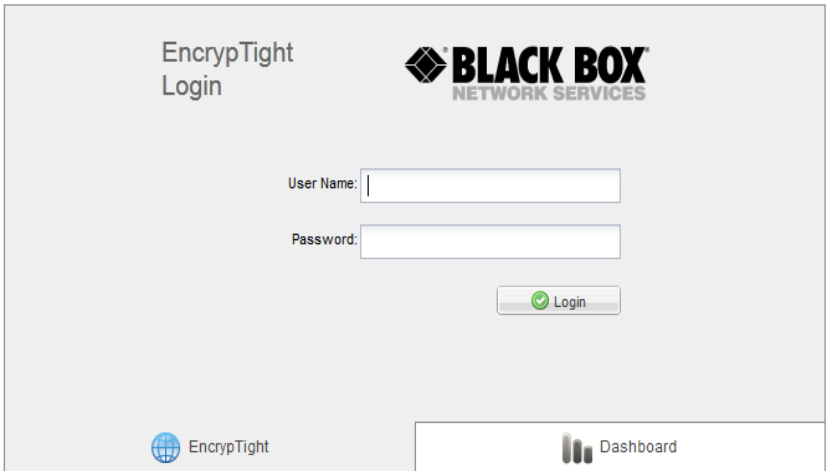


Figure 5 ETM Server Login (email)



Scalability up to 50,000 PEPs

UI scalability recommendations

- Use ETM UI for small/initial policy configuration:
  - Tree views, drag-and-drop, drop-down lists are easy to use, but don't work well at scale
  - Use these for initial configuration

- Use scripts with ETM REST API to extend policies to scale
  - ETM GUI uses a private REST API today
  - Public REST API will be exposed in ETM 3.5
- Use grid views to monitor/manage at scale
  - Grid views scale up to millions
  - Based on paged database views
  - PEP grid for initial PEP configuration
  - Policy, audit, task grids

Figure 6 EncrypTight Manager Scalability Guidelines

Configuration	Small	Medium	Large	XL	XXL
ETM Version	Standalone Edition Server Edition Hardware Server	Server Edition Hardware Server	Server Edition Hardware Server	Hardware Server	Hardware Server**
ETM Cluster nodes	1	1	2	5	10
CPU	Dual core Intel x64 Xeon 2 GHz, or equivalent	Quad core Intel x64 Xeon 2 GHz, or equivalent	Quad core Intel x64 Xeon 2 GHz, or equivalent	Quad core Intel x64 Xeon 2 GHz, or equivalent	Eight core Intel x64 Xeon 2 GHz, or equivalent
Memory	2 GB	8 GB	8 GB	8 GB	96 GB
Disk	80 GB	80 GB	160 GB	160 GB	640 GB
Management network connectivity	100 Mbps	100 Mbps	100 Mbps	100 Mbps	1 Gbps
SAs per PEP	100	200	200	100	100
Rekeys per day (for all policies, per PEP)	10	10	10	1	1
Maximum number of PEPs	**< 10**	**Up to 100**	**Up to 1000**	**Up to 10,000**	**Up to 50,000**

* See scalability assumptions for details (based on ETM version 3.5)

** Requires a special-order hardware server

Notes

- Scalability depends on configuration
- Scalability of up to 50,000 devices is feasible with 10 or fewer ETM servers, assuming reasonable design parameters
- ETM is architected to scale: main cluster and DR cluster, grid views, back end database, REST API (ETM 3.5)
- Black Box will improve scalability over time and will work with customers to meet and exceed required scalability
- These guidelines are intended to provide an engineering estimate of scalability for the most common deployment scenarios of Black Box customers. These guidelines are not a guarantee of performance or scalability for any specific deployment.

Assumptions

- Background polling: system default polling periods

- Checking status and config diffs: system default periods
- Are we collecting usage statistics? No
- The device types of the PEPs: ET0005A/ET0010A
- The new key install time: ETM 3.5/ETEP 2.3 with enhanced rekeying
- XL and XXL configurations assume a simple policy (100 SAs per PEP, with 24 hour rekeys)

REST API

The API exports a number of complex operations, such as policy deployment, rekeying, etc.

- Add or remove a ETVEP from an existing policy
- PEP call back to ETM to change address

API to support a mashup for EaaS service providers to allow the service provider's web portal to display a summary of the customer's service without logging into ETM

Complex Operations

The API exports a number of complex operations, such as policy deployment, rekeying, etc. These are documented below:

Pep Operations

- /api/pep/adopt : a POST request that adopts a PEP into the ETM management system.
- /api/pep/policyRules : a GET request that returns the latest policy and keys XML document for a given PEP, as identified by the serial number in the clientId. Note this variant can only be executed by a PEP. Only called by PEPs.
- /api/pep/{oid}/policyRules : returns the latest policy and keys XML document for a given PEP, as identified by the oid in the URL

Pep Certificate Operations

- /api/pep/generateCsr : a POST request to generate a new CSR and optionally sign and install it on the PEP.
- /api/pep/deleteCsr : a POST request to delete a PEP CSR.
- /api/pep/deleteCsr : a POST request to delete a PEP CSR.
- /api/pep/signCsr : a POST request to sign a PEP CSR and optionally install it on the PEP.
- /api/pep/getCertificate : a POST request to get a PEP Certificate.
- /api/pep/refreshCertificates : a POST request to refresh the list of PEP Certificates.
- /api/pep/installCertificate : a POST request to install an end certificate on the PEP to use as its identity certificate.
- /api/pep/installExternalCertificate : a POST request to install an external (trusted) certificate on the PEP.
- /api/pep/getCrl : a POST request to get a PEP CRL.
- /api/pep/deleteCrl : a POST request to delete a PEP CSR.
- /api/pep/installCrl : a POST request to install a CRL on the PEP.

Policy Operations

- /api/policy/activate : a POST request that activates a given policy, so that it will be included in any subsequent deployments.
- /api/policy/deploy : a POST request that performs a ETM deploy operation. Note that a deploy action is global. That is, the rules for all active policies are deployed together, but only to the PEPs that need to receive them (e.g. newly added Pep in an EasyMesh)

Enhanced fail-safe rekeying – avoids network splits

- We support two rekeying modes: time-based (current default) and enhanced fail-safe rekeying. The mode is configurable on a per-site basis (not per policy). Enhanced fail-safe rekeying is designed to delay the rekey rather than drop traffic in the data plane of the network. The reason for this somewhat strict tradeoff is fundamental to group keying – if one or more nodes that are participating in a group policy have a different key than the rest of the nodes in the network, then the network will be split, and data plane traffic will be dropped because traffic encrypted with one key cannot be decrypted with a different key (assuming symmetric encryption). Fail-safe rekey avoids this bifurcation of the data plane at the cost of possibly delaying the rekey. Fail-safe rekey is resilient to MITM attacks on the management plane in that data plane traffic is not affected by the attack, but it is vulnerable to a DOS attack against updating the keys.
- We also support a time-based rekey mode in which rekeys occur according to the strict rekey schedule specified in the policy. With this model, the rekey schedule is strict, so that even if some nodes have not received the new keys, the nodes that have received the new keys will stop using the old keys after a fixed time. The benefit of this is that it conforms to the strict rekey schedule, but the disadvantage is that when some nodes stop receiving on the old inbound keys, other nodes may not have received the new outbound key yet and in this case the data plane would be split. The time to start using the new outbound key (n) and the time to stop receiving on the old inbound key (m) are programmable, and ETM will keeps trying to send the key if it fails initially. The difference between m and n (m-n) is an overlap period that allows time to program new outbound keys throughout the network while still receiving on either the old or new inbound keys. Time-based rekey allows the nodes that are reachable to be rekeyed, but any nodes that are not reachable between time t and t+m will continue to use the old keys while the rest of the network is using the new keys, so the data plane will be split.

ETM Server Recovery

We have a new EncryptTight feature that allows customers to re-image their ETM server, returning it to the factory state. Customers can do this without shipping the servers back to Black Box. Black Box will deliver a DVD (or USB flash drive) to the customer, and they will follow a procedure to boot from the media supplied and then re-install the ETM server, returning it to the factory state.

Installation from DVD

You can now boot ETM from a DVD containing a policyserver-mediaboot-xxxx.iso on a Dell r310. Once booted it will automatically create a fresh ETM installation. When the installation is complete, the server is exactly like the pxeboot installation. You will still have to edit the policyserver-init.conf and run the policyserver-install.

Installation from USB

You can now also boot from a USB flash drive containing a policyserver-mediaboot-xxxx.iso on a Dell r310. Once booted it will automatically create a fresh ETM installation. When completed, the installation is exactly like the pxeboot installation.

- On a Dell r310 place the USB flash drive into an open slot on the front of the machine.
- When starting up the machine, press F11 to enter into the BIOS boot options.
- Select the USB device to boot from.

NOTE

The ETM Server Recovery feature is only supported in ETM version 3.5 and later. We do not support it for earlier versions of ETM.

System Requirements

Software Requirements

The minimum version of VMWare supported is ESX 4.0 update 1 (or higher), released in June 2010.

Browser Requirements

For optimal security, stability and performance, the latest major release of the following browsers are fully supported and tested on a rolling basis*:

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome™

* Earlier versions and unlisted browsers may be fully or partially supported.

Known Issues

Management Port Behavior

EncryptTight Manager must use 8443 as the default ETEP listening port for versions 2.3 or greater appliances and 443 for versions less than 2.3.

NOTE

When adopting pre-2.3 version ETEPs, you MUST ensure that the mgmt port is set to 443 instead of 8443 which is the new default for version 2.3 ETEPs. You can do this by either explicitly typing 443 in the Port field, or by selecting a previous software version in the PEP Software Version drop down, which will set the Port field to 443.

For known issues with a ETM release, please contact Black Box Technical Support.

Technical Support

Contact our FREE technical support, 24 hours a day, 7 days a week:

- Phone: 724-746-5500
- Fax: 724-746-0746
- e-mail: info@blackbox.com
- Web site: www.blackbox.com

Resolved Issues, Additions, and Modifications

The issues noted below have been resolved, added, and/or modified in EncrypTight Manager, v3.5.

[Issue-1229] - ETM REST API: installCertificate not working as expected on ETM v3.5.5757

[Issue-1228] - "Application Servers" property differs between ETM v3.5 and ETEP v2.3

[Issue-1227] - The PEP Alert Notification Configuration changes doesn't get reflected after going to a different tab and again viewing the change.

[Issue-1226] - User Created from ETM using IE :"Could not recognize your User Name or Password" throws the Error while Login using the details

[Issue-1225] - On ET1000A Under Data Port Settings you are not able to see Local and Remote Auto-Negotation settings.

[Issue-1224] - PEP import generates Java error on ETM v3.5

[Issue-1223] - Auto-Negotiation from ETM is not updating to ETEP.

[Issue-1222] - Reboot throws Exception during an Upgrade from 2.2-cust1 to 2.3.2

[Issue-1220] - PMTU: ETM (3.5) is sending dfIgnore="Enabled" when we set the reassembly to "Host mode"

[Issue-1218] - Cannot Deploy blank policy when the ETEPs are in Layer2 mode.

[Issue-1216] - Editing of Network Set throws " java.lang.NullPointerException" on upgraded ETM (3.4.5231-3.5.5740)

[Issue-1215] - Change "NAT IP Address" to "External IP Address"

[Issue-1210] - ETM must add a new configurable threshold for number of packets required for encryption alert status to change

[Issue-1206] - DVD and USB auto installation of ETM using kickstart just like PXE

[Issue-1204] - Global option to export ETM Config grid to Excel

[Issue-1190] - ETM must use 8443 as the default ETEP listening port for 2.3 or greater appliances

[Issue-1185] - Automatically refresh certificates when first contact is made to a pre-provisioned PEP

[Issue-1181] - Consider other places where ETM should use it's NATed IP address

[Issue-1178] - No log triggered in Audit Log/Task History when deleting an external certificate from a PEP

[Issue-1177] - L2 IKE encrypt policies to be defined as rekey encrypt policies type inside ETM Home Dashboard

[Issue-1175] - Add support for specifying an SSH port other than 22 for the PEP

[Issue-1172] - Add mgmtPort to the Add Pep form

[Issue-1171] - ETM alert for when a ETVEP goes oversubscribed and no is not longer applying it's policy

[Issue-1168] - Do not deploy to ETVEPs that are in an over subscribed state

[Issue-1164] - Add a Heartbeat Failure PEP status

[Issue-1162] - Enhance Diff Config to indicate differences that are "read-only" for ETM and therefore cannot be copied

[Issue-1151] - Add the ETM version and build number to the database backup file name

[Issue-1150] - Alert thresholds for the PEP should be in their own tab ("Alerts") (not in the Logging tab)

[Issue-1148] - Modify ETM installation to use TLS for the postgresql JDBC connection (for new installations only)

[Issue-1146] - Not Encryption alarm should provide more details about Percentage of Encryption against Thresholds under the details Column

[Issue-1145] - ETM must clear all alerts for a ETEP when pepd restarts - ETEP will send a clear all message

[Issue-1143] - ETM should allow users to control the safe mode behavior of appliances (pass in clear or drop traffic)

[Issue-1140] - Modify UpgradeProgressService to use the new information provided by the ETEP when an upgrade fails

[Issue-1121] - Add ability to have a Salt attached to the TransformData for algorithms that support it

[Issue-1111] - ETM must support reading an setting the following alarm threshold values for one or more PEPs at a time

[Issue-1099] - Enhance ETM installation to support having two ETM nodes with one (possibly external) database host

[Issue-1087] - Support AES-128 encryption for 2.3 appliances

[Issue-1080] - Edit Row function allowing NTP server update on a PEP

[Issue-1038] - ETM will allow users to enable usage of a VLAN for management traffic, and to specify the VLAN if enabled

[Issue-1031] - Add ETM support for configuring propagateTtl for MPLS polcies

[Issue-1029] - Three phase fail safe rekey

[Issue-1028] - ETM must allow users to configure the PEP heartbeat protocol

[Issue-1024] - Three phase rekey / failsafe ping configuration settings

[Issue-1022] - Add ETM support for requesting PEP Factory Reset

[Issue-1018] - Use new XML-RPC to get log files from the PEP and resurrect the "clear log files" option

[Issue-1017] - Allow SHA2 to be configured for 2.3 PEP CSRs

[Issue-1004] - Add archive (zip) support to the File Tree component

[Issue-1003] - Allow partial policy deployments for layer 2 mesh policies

[Issue-992] - TACACS+ ETM configuration for PEPs

[Issue-979] - ETM must expose the tunnel port to be used for traffic destined to a PEP, on the PEP Edit form, Remote Interface

[Issue-978] - ETM must supply a PEPs udp port in the tunnel endpoint element for policies that have rules to those PEPs.

[Issue-977] - Move policy validation checks to EJB layer (perhaps interceptor) for API

[Issue-974] - Delete Network and Network Set When Policy Is Deployed

[Issue-970] - ETM Must update the management address for ETEPs when it learns its IP Address has changed (via Heartbeat)

[Issue-966] - Two Factor Authentication using mOTP

[Issue-961] - Allow PEP configuration changes to be applied directly from the PEP Edit form

[Issue-936] - TACACS+ for centralized ETM authentication

[Issue-925] - ETM should provide indication if DR is up to sync with main site policies

[Issue-923] - ETM must notify peer ETEPs of tunnel endpoint changes

[Issue-918] - ETM should provide a flexible, configurable alert notification and reporting system

Related Documentation

EncrypTight Manager

- Black Box EncryptTight Manager Installation Guide
- Black Box TrustNet Manager User Guide

Encryption Appliances (PEPs)

- ETEP Enforcement Point, Installation Guide
- ETEP Enforcement Point, CLI User Guide

- ETEP Enforcement Point, Release Notes

Contacting Black Box Technical Support

Contact our FREE technical support, 24 hours a day, 7 days a week:

- Phone: 724-746-5500
- Fax: 724-746-0746
- e-mail: info@blackbox.com
- Web site: www.blackbox.com