Operation Guide

SYSCTL AB

Contents

Impex Operation Guide **4**

Definitions . . . 4

Contacts . . . 4

System overview **4**

Deployment Flexibility and Network Architecture **6**

Network with ICC and Repo installed on the same server in a basic network . . . 7

Network with ICC and Repo installed on separate servers in a zone based network . . . 8

Network for the DataLock . . . 9

Interaction Overview **10**

Client software requirements **10**

Accessing the ICC Application . . . 11

Performing Administrative Tasks . . . 11

Operation Description **11**

USB Protect and DataLock . . . 11

ICC and Repo Servers . . . 11

Definition Update Interval . . . 12

Password Usage in the Solution . . . 12

Passwords in USB Protect and DataLock . . . 12

Passwords in the ICC Server . . . 13

Passwords in the Repo Server . . . 13

Default Passwords . . . 13

Reset ICC Application Password . . . 13

Administrative Login . . . 14

DataLock SSH Configuration and Root Access . . . 14

Datalock destination test . . . 15

USBProtect Access . . . 16

Service Accounts . . . 16

Termination Procedures . . . 16

Service Window . . . 17

Certificate Management Overview 17
Using Let's Encrypt 17
Using an Internal or External CA for Certificate Management 17
Backup Strategy 19
Repository (Repo) Server Backup 20
ICC Backup Procedures 20
ICC Monitoring Overview 21
Syslog Overview for ICC and Repo 21
Remote Syslog Configuration 22
Running ICC and Repo in VMware 23

Impex Operation Guide

Purpose of This Guide

This operations guide is designed to support users in operating Impex systems. It provides both general and specific instructions related to the operation of USB Protect, DataLock, the ICC, and the Repo server. Please note that this guide does not cover the system or application architecture, which is detailed in a separate document. Additionally, troubleshooting procedures for USB Protect and DataLock are outside the scope of this guide and are documented separately.

Definitions

Word	Definition
Impex	The family name of USB Protect, ICC, Repo and DataLock
Stations	The family name of USB Protect and DataLock
ICC	The server which control the Stations and Datalocks
USB Protect	The kiosk computer used to scan mass storage devices
Repo	The server that has the updates and definitions
DataLock	Server used for network flows that will scan files before transferring them onwards
Network flows	This is the description of data being scanned and transferred through the DataLock to a remote destination. A DataLock can have multiple remote destinations configured
Operators	The users who will use the administrative interface on the ICC server

Contacts

Customers with an active support agreement are welcome to contact us via email at:

support@sysctl.se

System overview

System Overview: USB Protect and DataLock

USB Protect is a kiosk-based system designed to scan data on USB devices. Each USB Protect station is centrally managed by an ICC (Impex Control Center) server.

Key functionalities include:

- **File Scanning and Content Control:** USB Protect scans files on USB devices and enforces policy rules to allow or deny content based on predefined technologies.
- **Secure Communication:** All communication with the ICC server is initiated by the USB Protect stations over **TCP port 443**, using **TLS 1.3 encryption**.
- **Time and Configuration Management:** USB Protect retrieves its system time and configuration settings from the ICC server.

- **Log and Result Reporting:** Scanned data, operational logs, and other activity reports are pushed back to the ICC server.
- **Updates and Patching:** Engine definition updates, OS patches, and application upgrades are retrieved from a **Repo server**, which can either be hosted on the ICC server itself or on a separate dedicated server.

DataLock operates similarly to USB Protect, but instead of using USB devices, it handles file transfers over the network via **SFTP**. It supports scanning and transferring files through customizable workflows.

Infrastructure Components

- **ICC Server:**
  - Acts as the **central management** point for USB Protect and DataLock stations.
  - Exposes a secure **REST API** with authentication for communication with stations and potential third-party integrations.
  - Provides a **web interface** for system owners to manage devices and analyze results.
  - Supports configuration of key infrastructure settings such as **mail relay, DNS, NTP, and syslog**.
  - Local accounts are used by default, but integration with **Active Directory, Red Hat Identity Manager, FreeIPA**, or other **LDAP services** is supported for centralized identity management.
  - Admins can access the server via **SSH** or directly from the console.
- **Repo Server:**
  - Synchronizes engine definitions and updates from **updates.sysctl.se** over **TCP/443 with TLS**.
  - Hosts updates for distribution to stations.

System Architecture and Security

- All components (**USB Protect, DataLock, ICC, and Repo**) are based on **SYSCTL Linux**.
- **USB Protect and DataLock stations are locked down** — they are not intended for direct login or remote access.
- Configuration for these stations is managed centrally via configuration cards on the ICC server.

Deployment Flexibility and Network Architecture

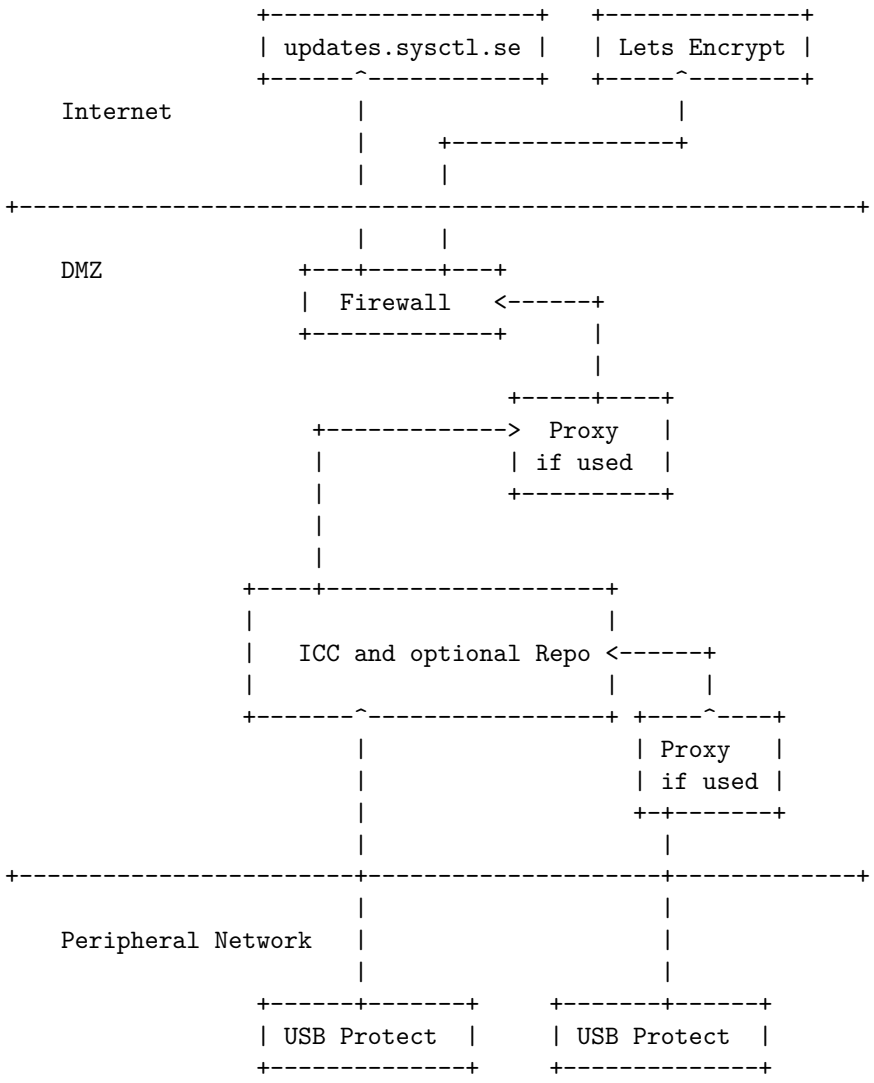
The Impex solution is designed to integrate seamlessly into network architectures that follow the **IEC 62443** standard and similar **zoned security models**, while also accommodating other network topologies.

Key deployment considerations include:

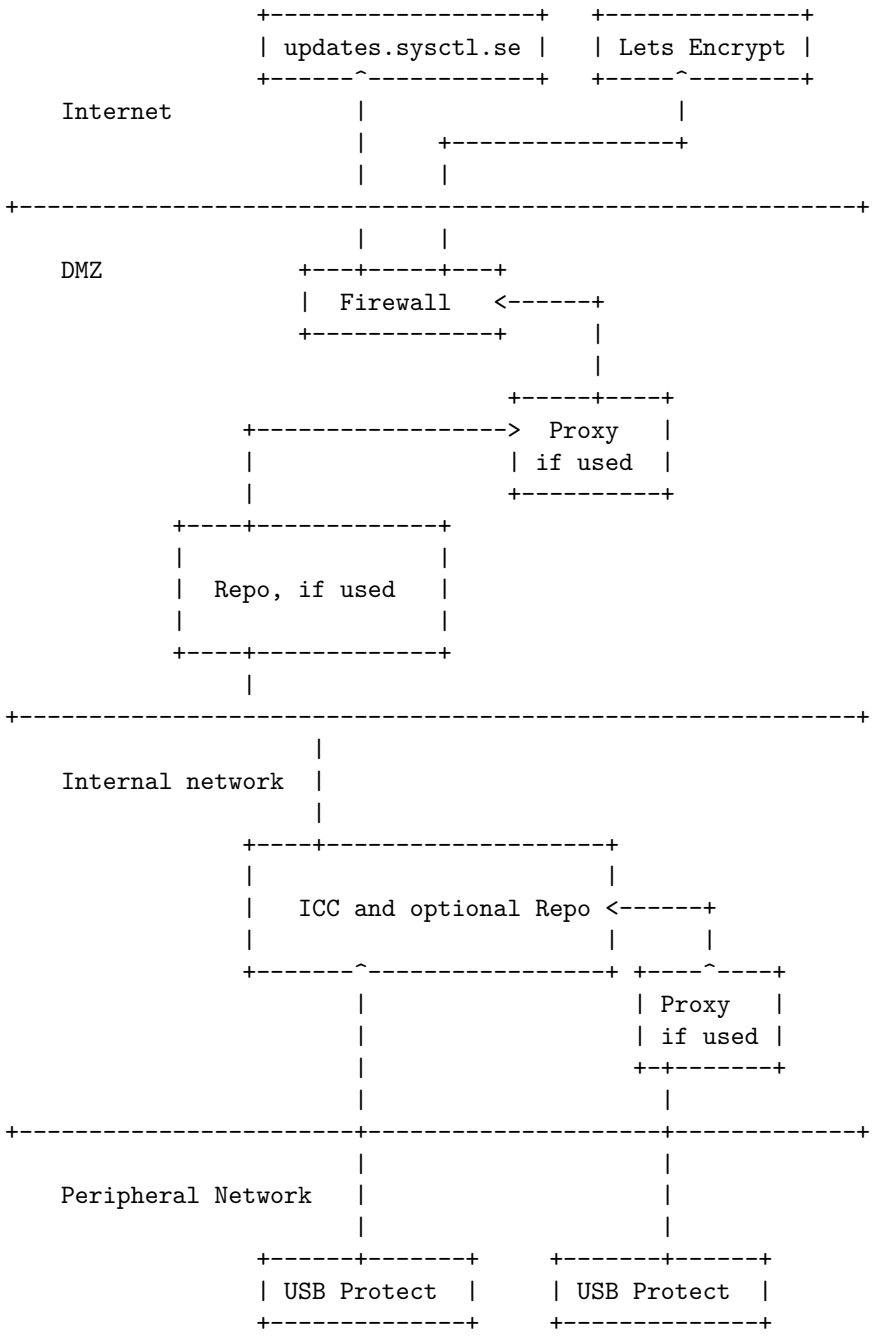
- **Flexible Deployment:** The ICC and Repo components can be hosted on the same machine; separate servers are not required.
- **Proxy Compatibility:** While the solution is fully compatible with the use of network proxies, the use of a proxy is optional and not mandatory for proper operation.

This versatility ensures that Impex can be adapted to a wide range of secure network environments and design preferences.

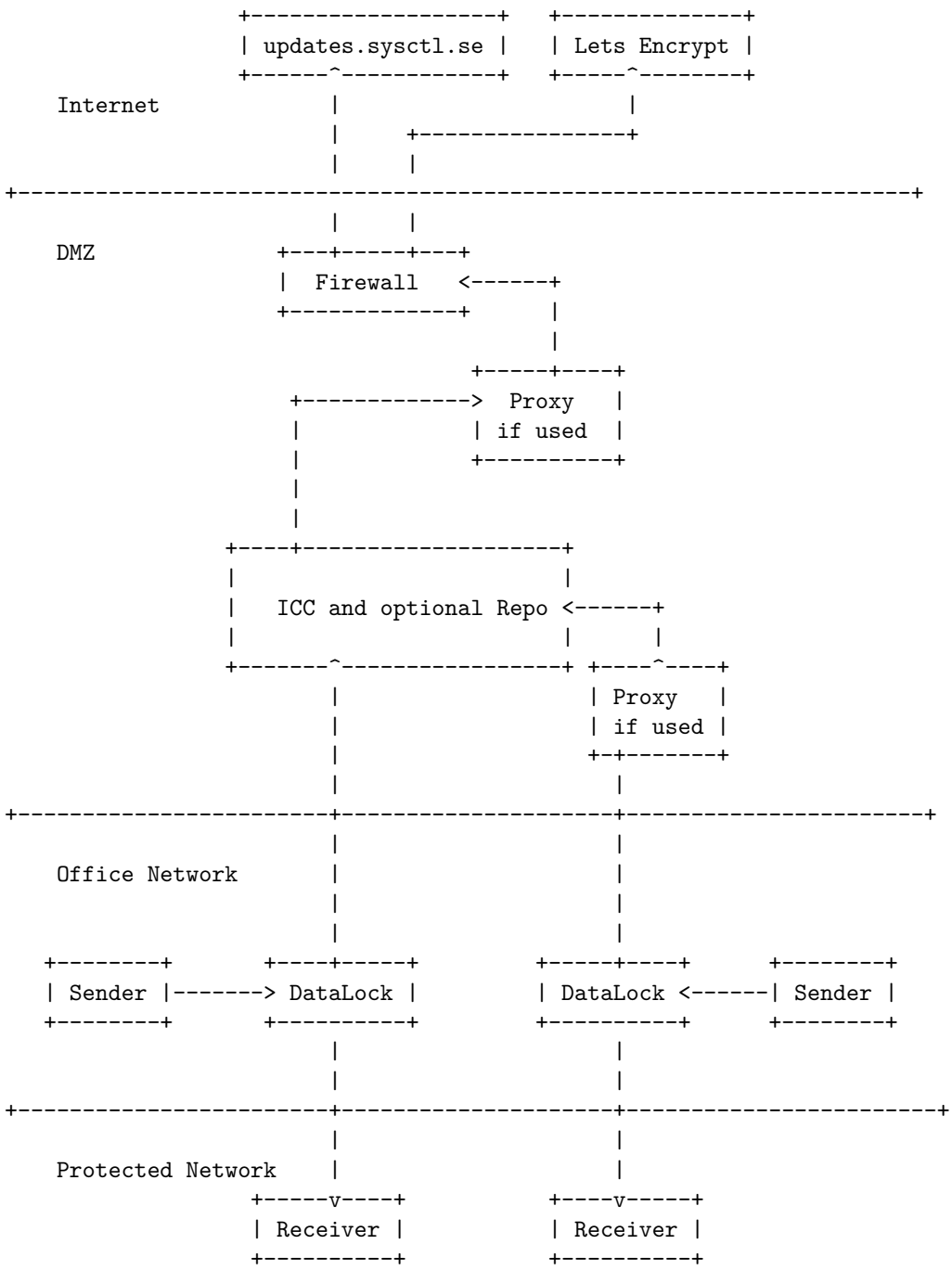
Network with ICC and Repo installed on the same server in a basic network



Network with ICC and Repo installed on separate servers in a zone based network



Network for the DataLock



Interaction Overview

The table explains the normal interactions used by the system, but it may differ depending on the actual installation if other integrations are used, like Active Directory. The table outlines the standard interactions within the system. However, actual implementations may vary depending on specific deployment configurations—for example, when integrations such as Active Directory or other external services are in use.

Data	Delivers to	Receives from	Tool	Protocol/ Port	Short Description
Mail	smtp.tld	ICC	Mail Relay	SMTP TCP/25	Information from ICC to end users
Time	ICC	ntp.tld	NTP	NTP UDP/123	Time source to ICC
Time	Repo	ntp.tld	NTP	NTP UDP/123	Time source to Repo
DNS	ICC	resolver.dns	DNS resolver	DNS UDP/53	DNS lookup for ICC
DNS	ICC	resolver.dns	DNS resolver	DNS TCP/53	DNS lookup for ICC
DNS	Repo	resolver.dns	DNS resolver	DNS UDP/53	DNS lookup for Repo
DNS	Repo	resolver.dns	DNS resolver	DNS TCP/53	DNS lookup for Repo
Logs	syslog.tld	ICC	Syslog	Syslog UDP/514	Sending syslog to log collector
Logs	syslog.tld	Repo	Syslog	Syslog UDP/514	Sending syslog to log collector
Updates	USB Protect	Repo	Patches/ Signatures	HTTPS TCP/443	Gets updates from Repo
Updates	DataLock	Repo	Patches/ Signatures	HTTPS TCP/443	Gets updates from Repo
Updates	ICC	Repo	Patches/ Signatures	HTTPS TCP/443	Gets updates from Repo
Updates	Repo	updates. sysctl.se	Patches/ Signatures	HTTPS TCP/443	Sync updates from sysctl
Cert	ICC	letsencrypt. org	Certificate renew	ACME TCP/443	Get certificate from letsencrypt
Cert	letsencrypt. org	ICC	Certificate renew	ACME TCP/80	Get certificate challenge from ICC

Client software requirements

The following software is required to manage and administer the Impex systems.

Accessing the ICC Application

To use the ICC web interface, a modern browser is required. The following browsers are supported:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Performing Administrative Tasks

To perform administrative tasks such as accessing the ICC or Repo server, an SSH client is required. Most operating systems include a built-in SSH client:

- **Windows:** Built-in SSH client (available via PowerShell or Command Prompt)
- **Linux:** Built-in SSH client (typically accessible via the terminal)
- **macOS:** Built-in SSH client (accessible via the terminal)

Operation Description

This section outlines routine and exceptional administrative tasks that may be required to maintain the Impex system components.

USB Protect and DataLock

These systems are designed to be self-maintaining, requiring no manual intervention during normal operation. They perform the following automated tasks:

- **Update Checks:**
  - System updates are checked **once daily**.
  - **Definition updates** (e.g., scanning engines or threat databases) are checked **every hour**, with a **randomized delay** of up to 30 minutes to distribute load across the network.
- **Scheduled Reboots:**
  - Both USB Protect and DataLock stations automatically **reboot once per week** to ensure optimal performance and stability.

ICC and Repo Servers

Routine administration for the ICC and Repo servers is minimal. However, the following should be noted:

- **TLS Certificate Management:**

  - If the **Let's Encrypt module** is **not** used, administrators must manually renew TLS certificates **before they expire**.
  - An **expired certificate** will prevent USB Protect and DataLock systems from receiving updates, potentially compromising system integrity and security.

- **Day-to-Day Operations:**
  - No additional daily administrative tasks are required under normal conditions.

Definition Update Interval

- **Sysctl Update Frequency:**
  - SYSCTL service retrieves and publishes updated definitions every hour, with the exception of **ClamAV**
  - The ClamAV upstream servers have **rate limiting** and are therefore updated **every third hour**.
- **Repo Server Synchronization:**
  - The Repo server checks for newly published definitions from **updates.sysctl.se once per hour**, with a **randomized delay of up to 60 minutes** to reduce simultaneous network requests across installations.

Password Usage in the Solution

This section outlines how **passwords are utilized and managed** within the solution architecture. It covers storage practices, authentication scopes, encryption considerations, and any integration points where password-based access is required. The intent is to ensure clarity on security posture, compliance with best practices, and operational awareness regarding sensitive credentials across system components.

Further subsections should be added to describe specific areas, such as:

- Web interface login
- API authentication
- Repository access controls
- Rotation and policy enforcement

Passwords in USB Protect and DataLock

- Each USB Protect and DataLock station is configured with a **randomly generated root password** during installation.
- This **root password is automatically rotated every day** to enhance security.
- The current password is stored securely and is **only accessible from the ICC server**.

Passwords in the ICC Server

After installation, the ICC server is configured with two separate passwords:

- `root` **Password (Operating System Access)**:
  - This password is **manually created** by the system owner during installation.
  - It is used for accessing the underlying SYSCTL Linux operating system.
- `admin` **Password (Application Access):**
  - The application's `admin` password is **randomly generated** during installation.
  - It is saved in the file: `/root/icc_admin`
  - This file is **readable only by the root user**, ensuring secure storage.
  - It is **strongly recommended** to **change the admin password before moving the system into production**.

Passwords in the Repo Server

- `root` **Password (Operating System Access):**
  - This password is **manually set** by the system owner during installation.
  - It is used to access the underlying SYSCTL operating system via console or SSH.

Default Passwords

- The **root password** must be **manually set during installation**. SYSCTL **does not have access** to or knowledge of this password.
- The `admin` **password** for the ICC application is automatically generated as a **random string** during installation and stored in:

`/root/icc_admin`

SYSCTL strongly recommends changing this password during or immediately after installation for enhanced security.

- The **USB Protect** and **DataLock** systems automatically **rotate their root passwords** daily. The current password is securely accessible only via the ICC server.

Reset ICC Application Password

To reset a user's password for the ICC application, SSH or console access is required. Use the following commands:

```
sudo -i

cd /opt/sysctl/impex-server/django-app

sudo -u impex-server ./manage.sh changepassword $username
```

Replace `$username` with the actual username of the account you wish to reset.

Administrative Login

Administrators can access the system either **locally via the server console** or **remotely using SSH**.

- By default, the **only interactive** user on the system is `root`.
- If additional users are created, they can perform administrative tasks using the `sudo` command. However, by default, `sudo` **will prompt for the root password**.
- To allow `sudo` access using **each user's own password**, the file `/etc/sudoers.d/users` must be modified accordingly.

Note: Always follow security best practices when modifying `sudo` permissions and restrict elevated access to trusted users only.

DataLock SSH Configuration and Root Access

Configuration File Location

DataLock uses its **own SSH configuration override file** located at:

```
/etc/ssh/sshd_config.d/60-datalock.conf
```

This file takes part in the **rule evaluation order** of OpenSSH's `sshd`, where configurations are **processed in lexical order**. That means:

- Lower-numbered files (e.g., `60-datalock.conf`) are evaluated first
- Higher-numbered files (e.g., `70-customer.conf`) override earlier rules if applicable

Default Restriction: Password Authentication

The `60-datalock.conf` file set

```
PasswordAuthentication no
```

This setting disables password-based logins **globally**, which enhances security by enforcing key-based authentication only.

Allowing Root Login (When Required)

In some cases, such as initial setup or certain troubleshooting scenarios, **SSH access for root might** be required. However, this must be done securely and explicitly.

Recommended Procedure

If SSH root login is needed, **do not edit `60-datalock.conf` directly**. Instead:

1. **Login via Station Token**

Use the **station token from ICC** to securely log in to the DataLock console.

2. **Create a custom override configuration**:

```
vi /etc/ssh/sshd_config.d/70-customer.conf
```

3. **Add the following content** to allow root login:

```
AllowUsers root
```

4. **Add an SSH key** to the root user:

- Place your public SSH key in:

```
/root/.ssh/authorized_keys
```

- Ensure correct file permissions:

```
chmod 600 /root/.ssh/authorized_keys
```

```
chmod 700 /root/.ssh
```

5. **Restart the SSH daemon** to apply changes:

```
systemctl restart sshd
```

Summary

Component	Action
Default Policy (`60-datalock.conf`)	Disables password auth globally (`PasswordAuthentication no`)
Override Recommendation	Use `70-customer.conf` with `AllowUsers root`
Root Login Enablement	Add SSH key to `/root/.ssh/authorized_keys`
Safe Practice	Never modify `60-datalock.conf` directly

Datalock destination test

To manually verify a Datalock destination, log in as **root** on the Datalock server and attempt to access the destination from the command line using the following command:

```
sftp server.tld -i /home/impex-outgoing/.ssh/id_rsa
```

Note: Adjust server.tld as needed for your environment

USBProtect Access

USB Protect supports only console access. See the USB Protect User Manual for more information

Service Accounts

- Each server includes a `root` account, which is configured during the initial installation.
- The **root password is manually set by the system owner** and is **not known or stored by SYSCTL**.
- **Post-installation Login Policy:**
  - No additional accounts are configured for system login by default.
  - **SSH login as `root` is disabled** for security reasons.
  - **Login is only possible via the local console** unless additional user accounts are configured.
- **Recommended Access Approach:**
  - **Personal user accounts** should be created for remote SSH access.
  - These accounts can then **escalate privileges using `sudo`**.
  - Personal accounts may be managed centrally via **LDAP services** such as **Active Directory, FreeIPA**, or **Red Hat Identity Manager**.
- To gain root privileges from a personal user account, use the following command:

```
sudo -i
```

Termination Procedures

Below are the commands for managing the Impex application and server operations:

Application Shutdown

To stop the Impex application:

```
systemctl stop impex-server
```

Application Start

To start the Impex application:

```
systemctl start impex-server
```

System Shutdown

To power off the server:

```
systemctl poweroff
```

Server Reboot

To reboot the server:

```
systemctl reboot
```

Service Window

The servers are configured to **automatically check for updates daily at 01:00** (local time), with a **randomized delay of up to 1 hour** to distribute load across systems.

- **Updates** include operating system patches, engine definitions, and other relevant components.
- **Automatic Reboot:** If a system reboot is required to complete an update, the server will reboot automatically during this window.

Note: Plan administrative work outside of this time window to avoid interruptions.

Certificate Management Overview

Scope

- Certificates are required only for:
  - **ICC server**
  - **Repo server** (only if a separate Repo server is used)

The method of installation and renewal depends on the **customer's PKI policies**.

Using Let's Encrypt

If your deployment uses **Let's Encrypt**, the following applies:

Automatic Handling

- Certificate installation and renewal are fully **automatic** if the `letsencrypt` module is installed.

Configuration Path

- Proxy-related configuration for Let's Encrypt is handled via the file:

`/etc/sysconfig/impex-letsencrypt`

Using an Internal or External CA for Certificate Management

Manual Renewal Required

When certificates are issued by:

- **an internal Certificate Authority (CA)**, or
- an **external vendor**,

Manual renewal is required.

Importing Certificates

If the certificate is created outside the ICC or Repo installation:

- One **must import** the certificate, including the **full chain** (leaf + intermediates + root).
- Ensure the files are stored according to the specified **Certificate Path**.

Creating Certificates On-Server

If the certificate is created **on the ICC** or **Repo server**, one can use helper scripts **after the initial configuration** is complete.

Steps:

1. **Copy and modify the OpenSSL config:**

```
cp /etc/pki/tls/openssl.cnf /root/openssl.conf
```

Edit `/root/openssl.conf` to include:

```
[ v3_req ]

basicConstraints = CA:FALSE

keyUsage = nonRepudiation, digitalSignature, keyEncipherment

subjectAltName = @alt_names


[alt_names]

DNS.1 = host1.domain.tld
```

2. Run the certificate generation script:

```
bash /opt/sysctl/impex-server/tools/cert.sh
```

- The script requires the server to have a **correctly set hostname**.
- Output:
  - `hostname.key` (private key)
  - `hostname.csr` (certificate signing request)
- Stored in:

Stored in:

```
/root/pki/_timestamp_in_epoch_/
```

4. The csr-file must be signed by a truseted CA
5. **If the signed certificate needs format conversion**, the script also provides helper commands for converting:

- DER → PEM
- PKCS7 → PEM

Renewing Certificates

To create a new Certificate Signing Request (CSR) for renewal:

```
openssl req -new -key "_path_to_private_key" -out "_path_to_new_csr" -config /root/openssl.conf
```

Once the certificate is **signed by the CA**, save the certificate and its full chain in the appropriate location, as described below.

Certificate File Paths

Defined in:

```
/opt/sysctl/impex-server/etc/apache/conf.d/cert.d/cert.conf
```

Default Locations:

- SSLCertificateFile -> /opt/sysctl/impex-server/etc/apache/certs/impex.crt
- SSLCertificateKeyFile -> /opt/sysctl/impex-server/etc/apache/certs/impex.key

Note: You may use different filenames if configured in `cert.conf`. It's common to name files using the **FQDN**.

Required Format:

- The certificate file (`SSLCertificateFile`) must:
  - Include the **leaf certificate** and **all intermediate certificates**, in correct order (leaf → intermediates → root).
  - Be in **PEM** format.

Backup Strategy

Server Snapshots

- Snapshots of the servers can be used as the **primary backup method**.
- These snapshots are suitable for capturing both configuration and state.

During each upgrade of the ICC software, the system:

- Automatically creates a local backup (snapshot) of the database.
- This provides a built-in recovery point without manual intervention. §

Repository (Repo) Server Backup

No Backup Required

- The **Repo server** does **not require traditional backups of**:
  - Repository data
  - Signature data

Reason: Sync with Sysctl

- The **Repo server can always resync** its full content from **SYSCTL**.
- As such, storing or backing up repository files locally is **not necessary**, reducing storage and administrative overhead.

ICC Backup Procedures

Application Data Storage

- The ICC stores all application data in a **SQLite** database located at:

```
/opt/sysctl/impex-server/django-app/db/db.sqlite3
```

Backing Up the ICC Database

To create a consistent backup of the database, use the following command:

```
sqlite3 /opt/sysctl/impex-server/django-app/db/db.sqlite3 .dump > new_backup_file
```

- This command:
  - **Exports the entire database** in SQL format.
  - Is ideal for creating a versioned or timestamped backup (`new_backup_file`).

Recommendation: Run this during low-traffic windows to ensure data consistency, or temporarily pause ICC activity if possible.

Backing Up Custom YARA Rules

If **YARA rules** are used, consider backing up custom rule files:

- Path:

```
/opt/sysctl/impex-server/django-app/upload/yara/custom
```

- Notes:
  - These files are uploaded by ICC administrators.
  - Depending on their origin (e.g. uploaded from another managed location), they **might already exist in other backups**.

Tip: You can add this path to snapshot jobs or file-based backup scripts for completeness.

ICC Monitoring Overview

Built-In Monitoring Features

The **ICC** has built-in capabilities to monitor:

- **USB Protect**
- **DataLock**

It can also be configured to **send email alerts** if either of these services goes **offline**.

Ensure that email notifications are properly set up in your ICC configuration to make use of this feature effectively.

External Monitoring Recommendations

To ensure high availability and reliability, it is recommended to use an external monitoring system (e.g. Nagios, Zabbix, Prometheus, etc.) to monitor the following aspects of both the ICC and Repo servers:

1. **Web Server Response**

- Confirm that the web server is responding to requests on expected ports (e.g., 80/443).
- Common checks include:
  - HTTP/HTTPS status codes
  - Latency or downtime alerts

2. **Certificate Expiration**

- Continuously monitor the **SSL/TLS certificate validity** to avoid unexpected expiration.
- Checks should trigger alerts **well before expiration** (e.g., 30 days notice).
- Tools like `check_ssl_cert`, Certbot's renewal monitoring, or external services can be used for this.

Summary

Component	Monitoring Type	Responsibility
USB Protect	Online status + Email alert	ICC internal
DataLock	Online status + Email alert	ICC internal
Web Server (ICC & Repo)	Availability check	External system
Certificate Expiry	Expiry threshold alert	External system

Syslog Overview for ICC and Repo

Malware Detection Alerts

When either **USB Protect** or **DataLock** detects malware in a scan report, the **ICC** generates a syslog entry in the following format:

```
Dec 24 15:00:00 icc journal: ICC WARNING [ICC:14] \
Station detected malware (https://icc.domain.tld/v/operations?byId=2)
```

Key Notes:

- The log includes a **URL to the specific scan report** on the ICC.
- It does **not contain sensitive data** — only an alert reference.

Remote Syslog Configuration

ICC Remote Syslog

- The **ICC application** supports remote syslog configuration.
- The setup process is documented in the **ICC manual**.
- Use this feature to forward ICC-generated logs (including malware alerts) to a central log system.

Repo Server Remote Syslog

For the **Repo server**, remote syslog forwarding must be manually configured on the console.

Step-by-Step Configuration

1. **Create config file:**

```
sudo vi /etc/rsyslog.d/remote.conf
```

2. **Add the following configuration:**

Replace:

- `target="IP_ADDRESS_OR_FQDN"` with the actual IP or FQDN of your remote syslog server.
- `protocol="tcp"` with `"udp"` if your remote server uses UDP.

3. **Apply the configuration:**

```
systemctl restart rsyslog
```

4. **Consult support before changing other values:**

For advanced customizations or tuning of retry behavior, buffering, etc., it is advised to contact **SYSCTL support**.

Summary of Recommendations

Component	Syslog Support	Action Required
ICC	Yes (documented)	Use ICC manual to configure remote syslog
Repo Server	Yes (manual setup)	Create and edit /etc/rsyslog.d/remote.conf
Malware Alert Log	Standardized format with report link	Automatically generated by ICC

Running ICC and Repo in VMware

Purpose of VMware Tools

Installing **VMware Tools** (specifically, `open-vm-tools`) enhances the VM's ability to:

- Report accurate status and metrics to **vCenter**
- Support **VM-level operations** such as graceful shutdowns, reboots, and resource tracking
- Enable **advanced monitoring and management** features in VMware environments

Installing `open-vm-tools`

The package should be installed depending on whether the ICC server uses a **local Repo** or SYSCLT **external Repo service**.

If the ICC Uses a Local Repo (including the Repo server itself)

Use this command:

```
dnf -c /var/impex_repo/local_fedora_impex.repo -y install open-vm-tools
```

This command leverages the local repository configuration file (`local_fedora_impex.repo`) provided by the system setup.

If the ICC Does Not Use a Local Repo

Use this command instead:

```
dnf -c /etc/yum.repos.d/impex.repo -y install open-vm-tools
```

This configuration accesses the standard remote Impex repository.

Post-Installation Step

After installation, reboot the server to ensure the `open-vm-tools` service starts correctly and begins reporting to vCenter.

Summary Table

Scenario	Command to Install VMware Tools
ICC/Repo server with local Repo	dnf -c /var/impex_repo/local_fedora_impex.repo -y install open-vm-tools
ICC without local Repo	dnf -c /etc/yum.repos.d/impex.repo -y install open-vm-tools

Don't forget to reboot the server after installation.