**amit aditya  
  
again changed  
  
SBI  
  
Belapur  
  
Nothing**

Standard Operating Procedure

On

**CERTInext**

Platform Engineering-II Department

Global IT Centre, CBD Belapur, Navi Mumbai

**Issue Date: 14/03/2024**

**Version 1.0**

Contents

[Document History 3](#_Toc161316446)

[Document Review 3](#_Toc161316447)

[Distribution List 3](#_Toc161316448)

**[1 Introduction](#_Toc161316449)** [4](#_Toc161316449)

**[1.1](#_Toc161316450)****[Purpose](#_Toc161316450)** [4](#_Toc161316450)

**[1.2 Version](#_Toc161316451)** [4](#_Toc161316451)

**[1.3 Document Review](#_Toc161316452)** [4](#_Toc161316452)

**[2](#_Toc161316453)****[Pre-requisites](#_Toc161316453)** [5](#_Toc161316453)

**[3](#_Toc161316454)****[Working on CERTInext](#_Toc161316454)** [6](#_Toc161316454)

**[3.1](#_Toc161316455)****[User Creation](#_Toc161316455)** [7](#_Toc161316455)

**[3.3 Department Management](#_Toc161316456)** [7](#_Toc161316456)

**[3.4 License Management](#_Toc161316457)** [7](#_Toc161316457)

**[3.5 Certificate Discovery](#_Toc161316458)** [8](#_Toc161316458)

**[3.5.1 SSL/TSL Certificate Discovery](#_Toc161316459)** [8](#_Toc161316459)

**[3.5.2 HSM](#_Toc161316460)** [9](#_Toc161316460)

**[3.5.4 Certificate Store](#_Toc161316461)** [10](#_Toc161316461)

**[3.5.5 Cloud Providers](#_Toc161316462)** [10](#_Toc161316462)

**[3.5.6 File System (SBI specific requirement)](#_Toc161316463)** [10](#_Toc161316463)

**[3.6 Interfacing with Email and SMS](#_Toc161316464)** [11](#_Toc161316464)

**[3.8 Key Management](#_Toc161316465)** [11](#_Toc161316465)

**[3.9 CSR Template Configuration Management](#_Toc161316466)** [12](#_Toc161316466)

**[3.10 Certification Configuration Management](#_Toc161316467)** [12](#_Toc161316467)

**[3.11 CA Connector Setting](#_Toc161316468)** [12](#_Toc161316468)

**[3.12 Manage Schedules](#_Toc161316469)** [12](#_Toc161316469)

**[4](#_Toc161316470)****[Network flow Diagram:](#_Toc161316470)** [13](#_Toc161316470)

**[5](#_Toc161316471)****[Data Flow Diagram:](#_Toc161316471)** [14](#_Toc161316471)

**[5.1 Internal CA Data Flow diagram](#_Toc161316472)** [14](#_Toc161316472)

**[5.2 External CA Data Flow diagram](#_Toc161316473)** [15](#_Toc161316473)

**[5.3 Key management Data Flow diagram](#_Toc161316474)** [16](#_Toc161316474)

**[6](#_Toc161316475)****[How can the user confirm if CERTInext is running](#_Toc161316475)** [17](#_Toc161316475)

**[7](#_Toc161316476)****[How CERTInextClient Works](#_Toc161316476)** [17](#_Toc161316476)

**[8](#_Toc161316477)****[Default port opening pre-requisite:](#_Toc161316477)** [18](#_Toc161316477)

**[9](#_Toc161316478)****[FAQs](#_Toc161316478)** [18](#_Toc161316478)

Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Created On | Version | Prepared by/ Changed requested by | Remarks (Brief Details of changes) |
| 14.03.2024 | 1.0 | Peyyala Subbarao | Initial Version |

Document Review

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Created On | Version | Reviewed By | Signature | Remark |
| 14.03.2024 | 1.0 | Shri Jignesh Solanki & Shri BHUVANESHWARAN PAGYASALI |  |  |

Distribution List

|  |  |  |  |
| --- | --- | --- | --- |
| Version No | Date | Distributed to | Purpose |
| 1.0 | 14.03.2024 | All Departments under GITC | SOP for CERTInext |

# **1 Introduction**

As part of ECKMS Solution, to handle the Certificate Life cycle and to Discover all the certificates in the network enterprise, CERTInext is designed to provide clear and detailed instructions to discover, Configure, deploy certificates. The CERTInext application is used to scan hostnames and IP addresses to discover certificates. The discovered certificates can be found in the Manage Certificates page, where users can view the status of the certificates, check expiry details, configure, initiate, order, and deploy certificates.

CERTInext offers discovery and deployment options to various Use cases such as

1. Tomcat Server.
2. JBoss Server.
3. Jetty Server.
4. IIS Server.
5. Ngnix server.

However, in this Document we will be discussing Tomcat Server as at SBI we have deployed CERTInext on the Tomcat Server.

## **Purpose**

To scan hostnames and IP addresses to discover certificates. The discovered certificates can be found in the Manage Certificates page, where users can view the status of the certificates, check expiry details, configure, initiate, order, and deploy certificates. Also, to display the consolidated report of certificates on the Dashboard.

## **1.2 Version**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Author** | **Status** | **Revision Details** |
|  | 1.0 | Subbarao Peyyala | Draft | Initial Draft |

## **1.3 Document Review**

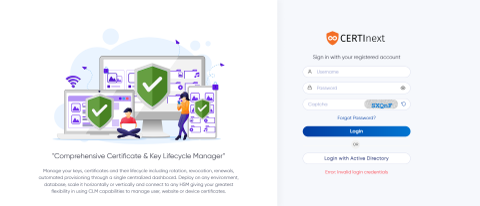
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Created On** | **Version** | **Reviewed By** | **Signature** | **Remark** |
|  |  |  |  |  |

# **Pre-requisites**

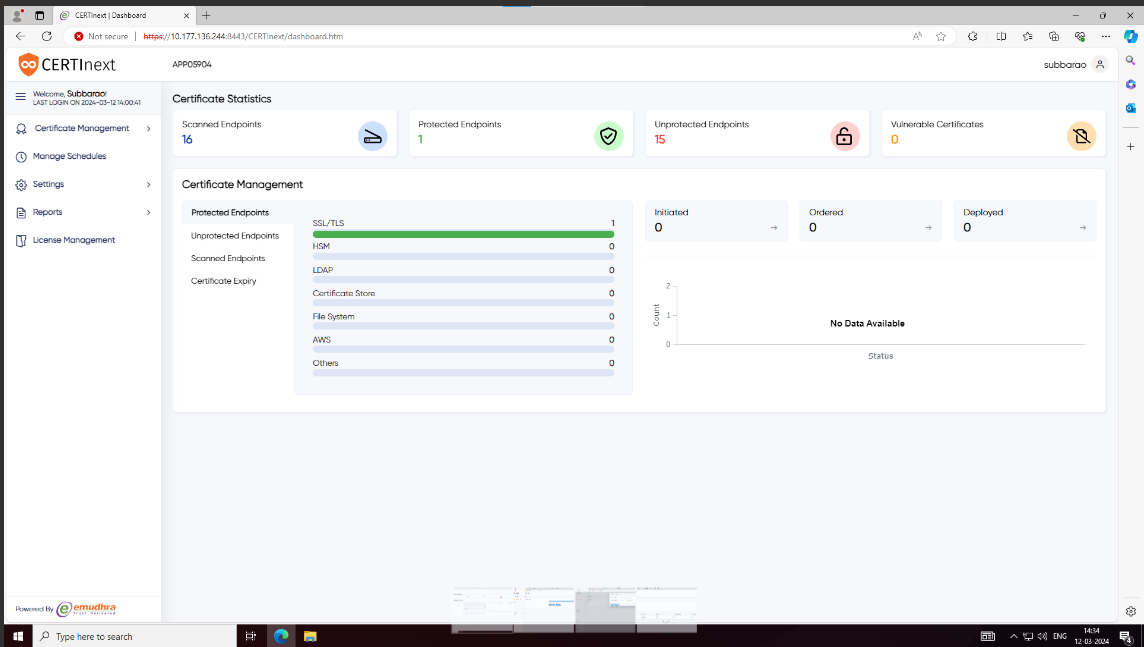
At least one server available to run CERTInext and another server to run the CERTInextClient. However, both CERTInext and CERTInextClient can run on the same server.

The creation of an admin is a prerequisite for CERTInext. Different CERTInext tasks will be carried out by a user with admin access.

* User needs login to CERTInext as a “Superadmin” user.



* User opens login page.
* User enters their “username” & “password” in the designated field.
* User enters the “captcha” in the designated field.
* User clicks the “login” button.
* The system validates the entered information.
* Upon successful login, the dashboard page appears as seen below.



* User logs into their superadmin dashboard page.

# **W****orking on CERTInext**

In SBI, eMudhra has CERTInext deployed on-premise. Also, emCA eMudhra’s Certifying Authority application is capable of issuing digital certificates to human as well as devices which is also deployed at SBI on-premise. Both emCA and CERTInext work together to Manage and Maintain Digital Certificates inside SBI enterprise.

* Dashboard
* User Management (Permission/Hierarchy)
* Certificate Management (Discovery/Editing/Tagging)
* Certificate Life cycle management
* Department Management
* License Management
* Interfacing with Email and SMS
* Customized Reports
* Key Management
* CSR Template Configuration Management
* Certification Configuration Management
* CA Connector Setting
* Manage Schedules

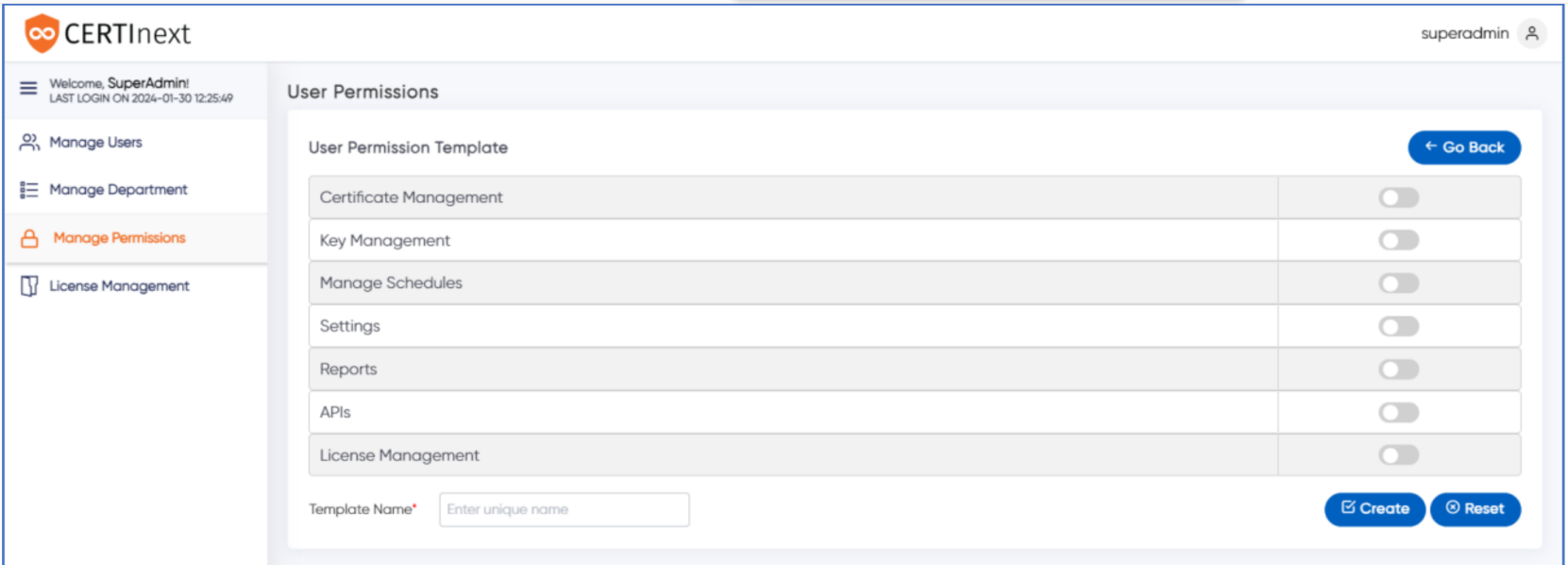
## **User Creation**

CERTInext supports creation of two type of users:

1. Superadmin
2. User (Role based)

The "Manage Users" page in the CERTInext application is a centralized interface designed for superadmin user to oversee and administer user accounts efficiently. The page will present user details in a tabular format, facilitating quick reference and management.

User with superadmin privileges can create as many users as he wants. Depending on the permissions any user needs, a ROLE template is needed to be defined first. User can be created by assigning the “Permission Template” to the user. The privileges of the new user created will be as per the permissions given in the Permission Template”.



This feature of CERTInext give the organization the flexibility to create users with customize privileges.

## **3.3 Department Management**

In the Manage Department, the super admin can add new departments and assign applications to these departments which enhances the flexibility and organization of user access and certificate management. New Department can be Added along with the Application Name which belong to that department.

Department can be Delete/Edited/Searched.

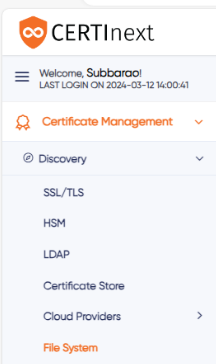
## **3.4 License Management**

The License management section in the Super admin portal of CERTInext allows users to effectively manage their CERTInext License. The Super admin User can renew the CERTInext Enterprise license. The "Generate ID" and "Register License" button will become active 30 days before the license expiration date.

## **3.5 Certificate Discovery**

CERTInext discovers digital certificates from devices and applications across enterprise data centers and multi-cloud environments. It supports both authenticated and un-authenticated scan of devices and applications for certificates. Enterprise can feed the CERTInext with IP Addresses or IP Addresses range along with ports for discovering certificates.

CERTInext has the capability to continuously scan the network for new certificates. User employs “SSL certificate discovery” method to discover certificates from “Tomcat server”.

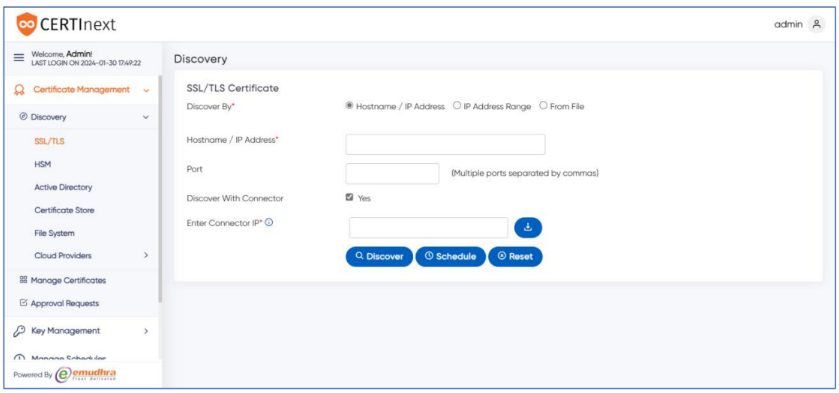


CERTInext user have the privilege to discover certificates of 6 different ways.

## **3.5.1 SSL/TSL Certificate Discovery**

* Discovering SSL/TSL certificates from a “Tomcat server”.

➔ The user selects the "Discovery" -> "SSL/TSL" tab in the left navigation.

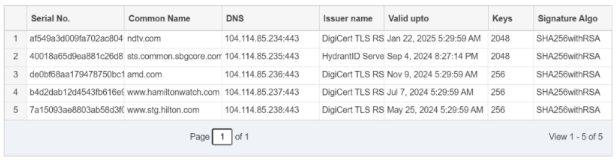


➔ By default, the "Hostname/IP Address" option is selected.

➔ The user enters the “Hostname/IP Address” of the respective device or web server.

➔ The user clicks the "Discover" button.

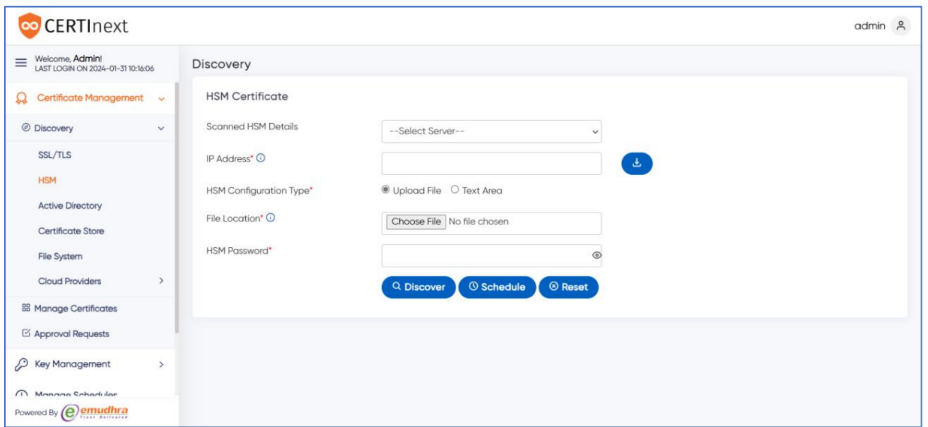
➔ The below page appears, displaying the discovered SSL certificates.



➔ The user can click the "Reset" button to re-enter the fields and initiate a new discovery.

User can discovery certificated using other discovery options:

## **3.5.2 HSM**

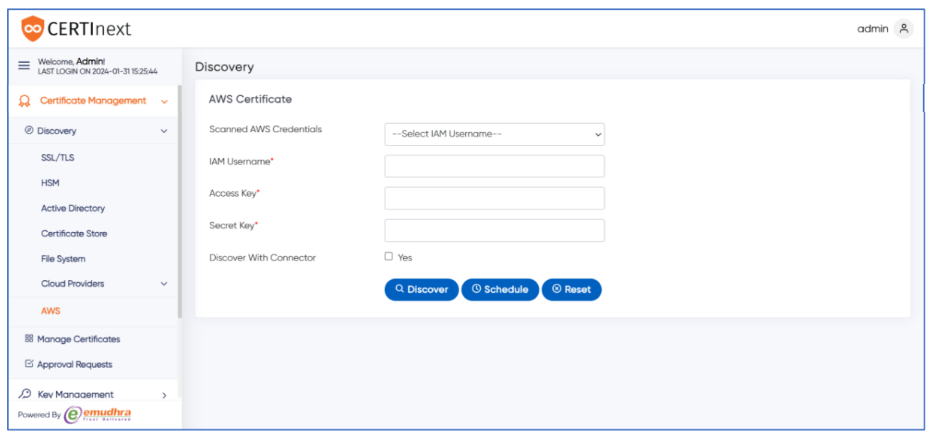


## **3.5.4 Certificate Store**

CERTInext user connects to the Windows machine of the given Host IP and import the certificates from the certificate store and lists them on the page.

## **3.5.5 Cloud Providers**

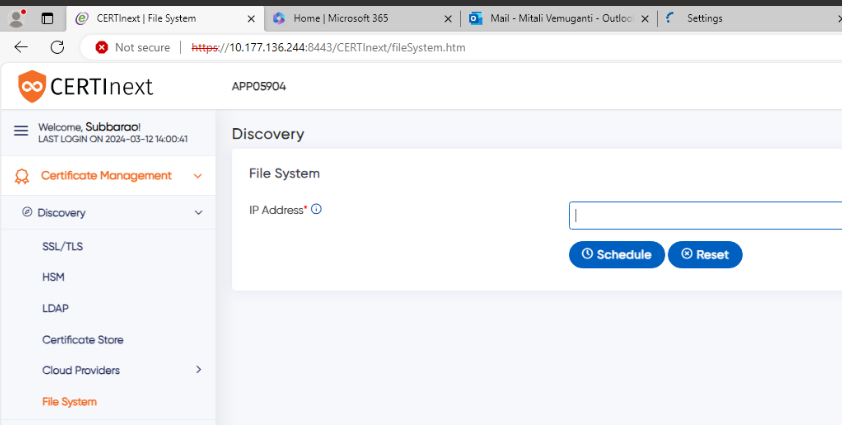
To discover the AWS Certificate users need to select the Cloud Providers → AWS submenu. The below image will be displayed

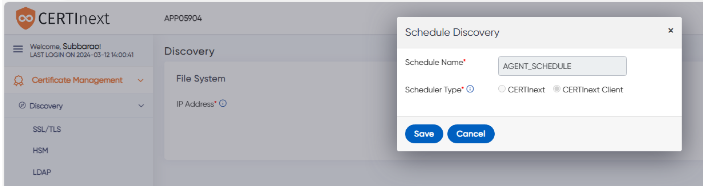


## **3.5.6 File System (SBI specific requirement)**

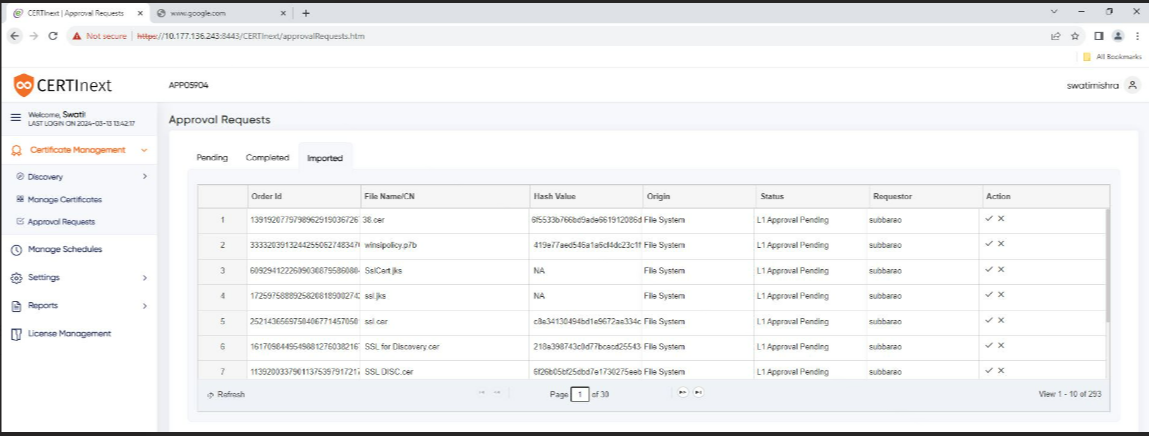
The CERTInext application facilitates certificate discovery from the “File system”, providing users with an efficient method to scan Servers for certificates. Users should select the “File System” sub-menu from Discovery menu.

* Enter the IP address of the target server or system into the designated field.
* Users should select the "Schedule" button
* A task is schedules to scan the File System.





* To view the certificate scanned, the User should select Certificate Management -> Approval Request to see the list of certificates which are found on the Server. User needs to click on the “Imported” tab to see the list of scanned certificates.



Under Imported tab all the scanned files are displayed

## **3.6 Interfacing with Email and SMS**

CERTInext allows Email and SMS customization. Allow more than one email-ID to be integrated with one application and provide can leverage to central admin to modify/add/delete the email IDs.

## **3.8 Key Management**

CERTInext is an advanced centralized key management system crafted to simplify the process through key distribution across a wide range of applications. CERTInext manages the entire lifecycle of symmetric and asymmetric keys, supporting resilient business processes and ensuring effortless compliance with both internal and external audits. Take charge of cryptography and achieve compliance through the centralized and automated application key management offered by CERTInext.

CertiNext Key Management comes with KMIP support to help you automate key management straight from CertiNext and ensure your ecosystem is always secure. CERTInext’s Key Management System (KMS) empowers to securely discover, manage, and utilize keys across various platforms within CERTInext environment.

CERTInext discovers both symmetric and asymmetric keys from devices like Hardware Security Modules (HSMs). It can also discover SSH Key and Keystore

The user can Create / Download / Rotate / Delete Keys

## **3.9 CSR Template Configuration Management**

Certificate Settings will include CSR Templates Settings and Configuration Templates Settings.

CSR Template can be Created / Edited / Cloned / Disabled / Enabled / Deleted

## **3.10 Certification Configuration Management**

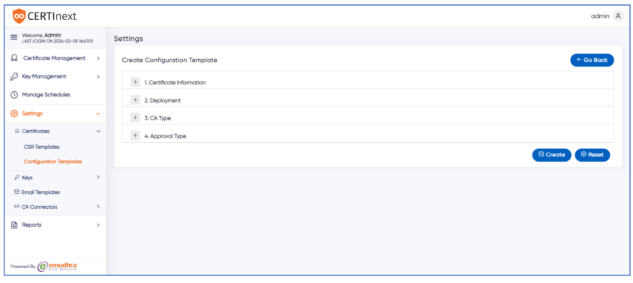
CERTInext allows user configure Certificate Template which will include configurable fields:

• Certificate Information

• Deployment

• CA Type

• Approval Type



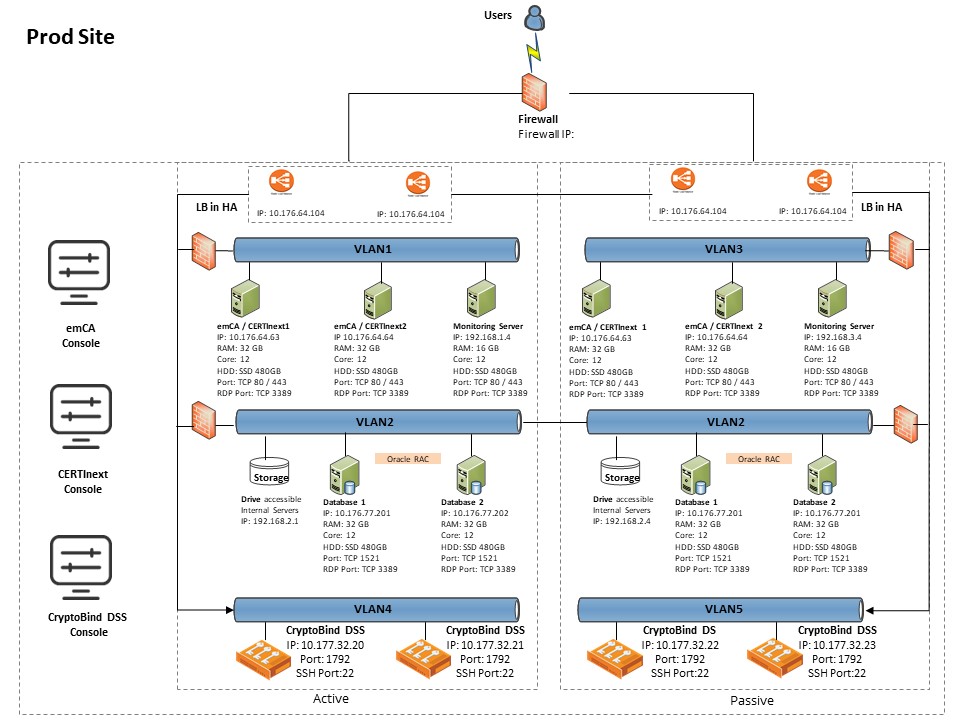
## **3.11 CA Connector Setting**

## **3.12 Manage Schedules**

CERTInext application offers an Automate Schedule feature that allows users to automate their Certificate Discovery, Notification, Deployment, and Rotation processes.

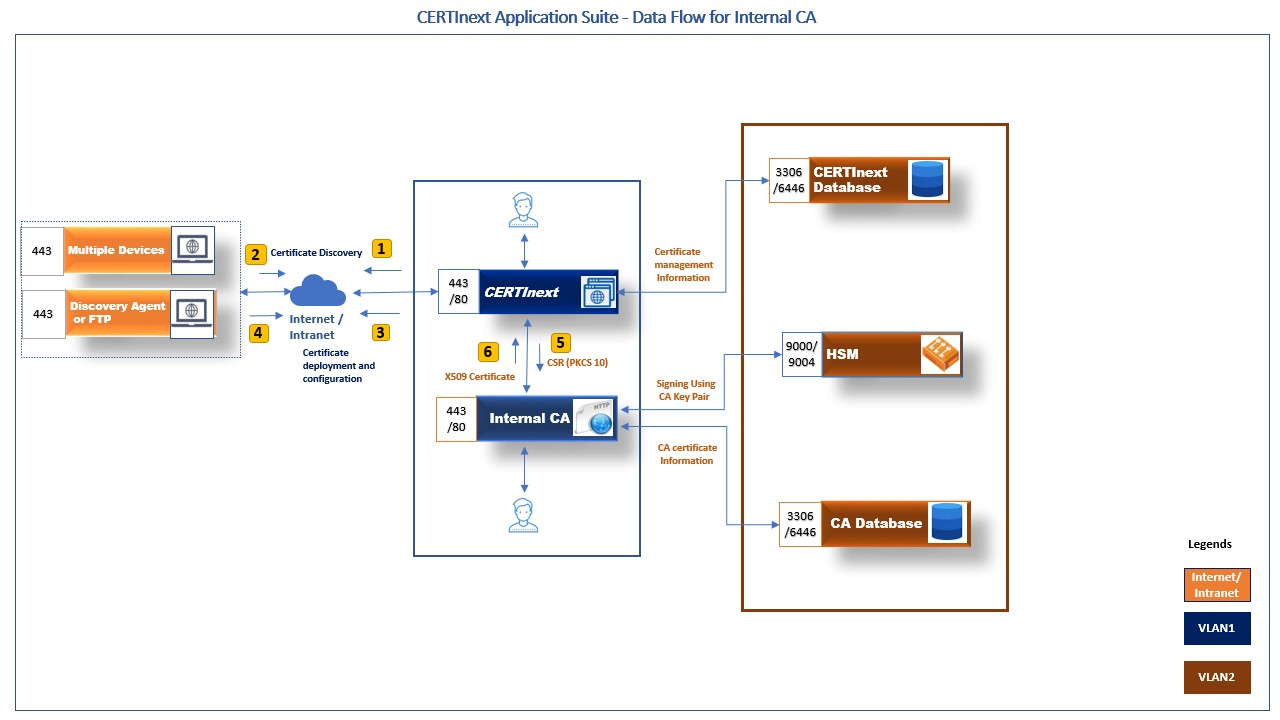
User can manage schedules displayed as a list on the manage schedule page. In the list of all the available schedules user can perform actions such as Edit, Disable,Enable, and Delete.

# **Network flow Diagram:**



# **Data Flow Diagram:**

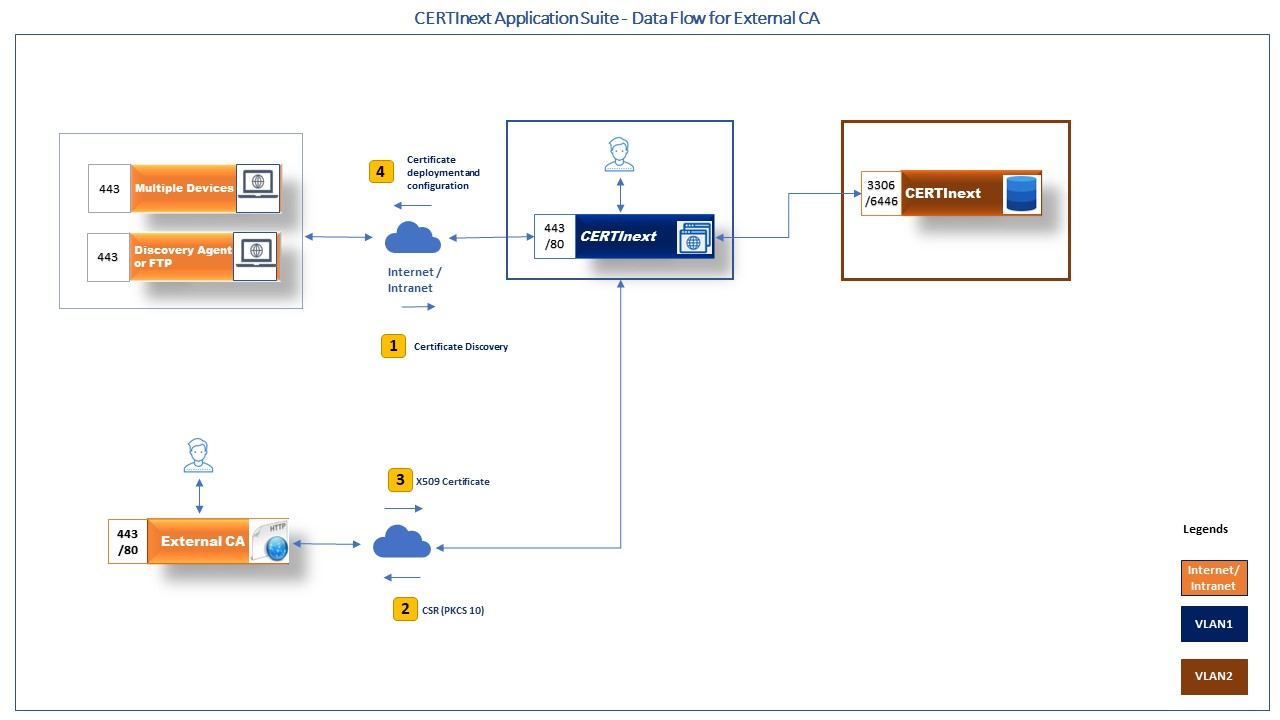
## **5.1 Internal CA Data Flow diagram**



The high level CERTInext data flow is explained below.

* User Login into the CERTInext admin portal
* Navigate to the certificate discovery option in the side menu of the dashboard page.
* Select SSL certificate discovery and enter the hostname/port number.
* With the help of a discovery agent or FTP, CERTInext will discover certificates from multiple devices.
* Admin should create certificate configuration template.
* User Login into the CERTInext officer portal
* Upon successful configuration of the certificate, officer will initiate, order and deploy the certificate.
* CERTInext is connected to the internal CA application and will provide the CSR (PKCS 10) and receive the X509 certificate.
* The internal CA will fetch certificate information from the CA database.
* The internal CA connected HSM will use the keypair for signing.
* CERTInext will store certificate information in the CERTInext database for management.

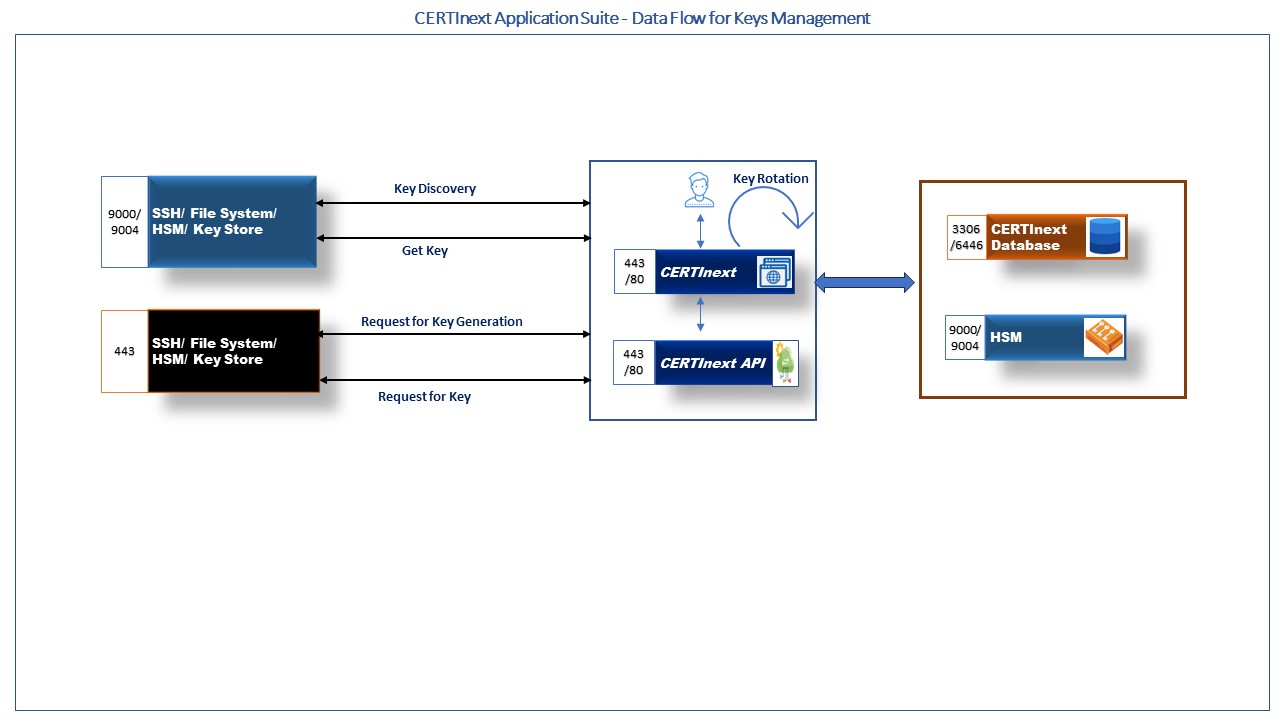
## **5.2 External CA Data Flow diagram**



The high level CERTInext data flow is explained below.

* User Login into the CERTInext admin portal
* Navigate to the certificate discovery option in the side menu of the dashboard page.
* Select SSL certificate discovery and enter the hostname/port number.
* With the help of a discovery agent or FTP, CERTInext will discover certificates from multiple devices.
* Admin should create certificate configuration template.
* User Login into the CERTInext officer portal
* Upon successful configuration of the certificate, officer will initiate, order and deploy the certificate.
* CERTInext is connected to the external CA application and will provide the CSR (PKCS 10) and receive the X509 certificate.
* The internal CA will fetch certificate information from the CA database.
* The internal CA connected HSM will use the keypair for signing.
* CERTInext will store certificate information in the CERTInext database for management.

## **5.3 Key management Data Flow diagram**



The high level CERTInext data flow is explained below.

* User Login into the CERTInext admin portal
* Navigate to the key discovery option in the side menu of the dashboard page.
* To discover keys, choose any discovery type (SSH, HSM, or Keystore) and provide the required information.
* CERTInext will discover keys.
* To create new keys admin should create key profiles for symmetric or asymmetric keys.
* User Login into the CERTInext officer portal
* Key profiles can be used to create new symmetric or asymmetric key.
* User can rotate keys or use newly generated keypairs to generate new certificates.
* To generate new keys from HSM CERTInext will connect to HSM.
* For SSH discovered keys can be used to map users and enable file transfers through SSH.
* CERTInext will store key information in the CERTInext database for management.

# **How can the user confirm if CERTInext is running**

* When CERTnext url is hit and the “login page” appears – we know that the service is up and running.
* Once login is successful using the login credentials, the user is allowed to navigate through the pages as per the “Permission” assigned to the user.

# **H****ow CERTInextClient Works**

When CERTInextClient works as an Agent. This agent helps CERTInext to search for the certificates in the Network and search for certificates in the entire File system.

The user can run the CERTInextClient using the procedure below.

1. Check if the port on which the CERTInext client should be listening is Free.

Command: netstat -ano | findstr :<port no>

Steps to run CERTInextClient JAR:

1. Create a folder where you want the certificates scanned to be stored. (ex: F:\Certificates)
2. Paste the CERTInextClient.jar in another folder in the server.
3. Open CERTInextClient.jar using 7-zip and go to path "\BOOT-INF\classes\".
4. In "application.properties" file change below 3 parameters:
   1. “certFolder.path" which will be the path of the folder created in step 1.

#Certificate Folder Path

certFolder.path=D:\CERTInext\ScanCertficates

1. “certinext.url" which will be the URL of the CERTInext.

  certinext.url=http://10.177.136.224:8080/CERTnext

1. “certinextclient.port" which will be the port number on which CERTInextClient will run.

certinextclient.port=<free port>

1. Paste "log4j.xml" in the folder which CERTInextClient jar is present and edit the path inside the file.
2. Create another folder named "logs" inside the folder where CERTInextClient jar is present.
3. Now run "cmd" as administrator and navigate to the path where CERTInextClient jar is present and run the following command "java -jar CERTInextClient.jar".

# **Default port opening pre-requisite:**

Below mentioned basic ports must be opened from your source system to ensure proper to efficiently manage the software/product.

Production Servers

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr No. | Source | Destination | Port | Direction | Notes |
| 1 | DC IP’s | Client Server | 8096 | Bi-directional |  |

DR Servers:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr No. | Source | Destination | Port | Direction | Notes |
| 1 | DR IP’s | Client Server | 8096 | Bi-directional |  |

# **FAQs**