CASE STUDY

# A Smart City Project in UTTAR PRADESH

ProcessIT Global

## Overview

The Government of India introduced an Urban renewal and retrofitting program with the mission to develop smart infrastructure within cities across the whole country, to make them citizen friendly and sustainable.

The Union Ministry of Urban Development is responsible for implementing the mission in collaboration with the state governments. The mission initially included 100 different cities, with the deadline for completion of the projects set between 2019 and 2023. The effective combined completion of all projects as of 2019 is at 11%. As of March 2022, 3577 projects out of total 6939 tendered projects have been completed, utilizing ₹60,073 crore out of total tendered amount of ₹191,294 crore.

## Challenge

Identity and access management was a key aspect of this project to provide a unified infrastructure across all the IOT ecosystem. It was a necessity to ensure data security within the organization as the project operates within critical and highly impactful confidential data.

All the users belonging to different subsidiaries of the project needed to be created within one unified solution, thus their access, and authorities can be monitored to ensure data security across the platform. Role based access needed to be granted to the users to ensure they can access the resources of the project as per their authorities. The user access sessions needed to be captured and monitored to make the platform less prone to breaches.

## Solution

PITG was chosen to implement a full identity and access management stack across one entire segment of the prestigious project, to meet the specific needs.
Implementation of Identity Manager was done to manage the user life-cycle. All of the users belonging from different project subsidiaries, were provided with one unified master identity and passwords. So, their access can be authorized on the network. Password management policies were employed, such as password strength assignment, periodic password change, and password blocking after several failed attempts to ensure enhanced security.

Implementation of Access Manager was done to provide single sign-on access to all web-based applications with multi-factor authentication via tokens.

Implementation of Advanced authentication was done to provide multi-factor authentication, as an extra layer of security while login into the user account.

Privilege account management solution was implemented to provide access to all servers, to the users through a single unified portal. users were segregated based on access group/policy, to get access to the list of available servers as per their authorities. The auditors were enabled to perform monitoring like Viewing server access session logs, keystrokes, screenshots of the session and even download reports through the solution.

## Results

Successful implementation of the solutions in the project environment secured it from the vulnerabilities controlled in an efficient manner.

***User management:*** All the users engaged with the project belonging to different infrastructure domains were managed through one unified portal, which made the system more automated and secure.

***Better Access control:*** User access was granted based on their authorities to ensure privilege-based access to the project resources.

***Enhanced governance:*** The user sessions were governed through real time monitoring mechanism, to make the system more secure, and protected from internal threats making it less Vulnerable