International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

One Touch Teams Room on Windows (MTR-W) Provisioning Automation

Ramesh Lakshmikanth

Unified Communications Engineering
rameshkl007@gmail.com

Abstract

In modern hybrid enterprises, especially working at a large-scale needs rapid deployments and collaborative infrastructure. The systems require embedded security, platform specific customization from the outset and access infrastructure. The paper talks about ZTP - Zero Touch Provisioning architecture that helps the system to be ready for deployments according to the company needs with negligible manual intervention (zero-touch) or a single step involved provision (one-touch). We aim to customize systems that come with a pre-installed setup tailored to the company's environment, minimizing the needs for repeated authentication, two- factor verification for access, and manual software installations. This approach includes close collaboration with the vendors like Lenovo, Dell, etc. and configuration provided by the company. As a result, companies can provide infrastructure ready systems that have strict security provisioning and less access requirements with frictionless user experience.

Keywords: Zero Touch Provisioning (ZTP), Microsoft Teams Rooms (MTR), Workspace ONE, Resource Account, Dropship Agent, Pre-configured systems, One touch deployments, IT Automation, Endpoint Security

I. INTRODUCTION

Imagine having a system with pre-configured setup, ready to fulfil the needs of an organization from the moment it is initially started. No lengthy installations by IT admins, no complex navigation, no time taking login process, this is not an advanced thinking or innovative outlook but an operational reality being implemented by Zero Touch Provisioning. Whether It's a Teams room device or a field laptop for an employee, every system should have rigorous security standards, certain configuration policies and meet application requirements. However, the traditional method used, had a lot of friction involved from user authentication to license assignment like multiple teams and system coordination which includes potential delays and more faults.

One Touch Provision flips this script for a better user friendly approach. This setup introduces a model where the system is initially loaded with customized operating systems, built in collaboration by the vendor, so that each device has embedded company's specifications. From disabling unnecessary two-factor authentication for resource accounts unlike the personal accounts, One touch provisioning makes deployments nearly negligible. Behind this smooth transition lies powerful orchestration services like PowerShell Automation, Workspace ONE and ServiceNow APIs that handle everything.

This architecture explains the implementation of such a system- that minimises human role and enhances operational efficiency. Through this system we are able to uncover how vendor collaboration, automation and system intelligence converge to build a strong solution with minimal error, reduced provisioning time and streamlined security services.

II. Problem Statement

In an industry, provisioning a new system is not like handing over devices and expecting them to start working. There is a standard setup working at the backend which is complex, error prone and often manual which may be inefficient and with high security risks. Whenever somebody joins an organisation, the company usually issues a system that has its base operating system. Then the IT administrators will configure user IDs, assign specific passwords, set up multi-layered authentication, and install team-specific tools and software applications.

At a large scale- where each employee needs assistance for the deployment, this can cause different challenges:

- Security Risks: The standard protocol involves the credentials, access and configuration to move within teams that may open risks for data leaks and unauthorised access.
- Poor User Experience: Repeated hurdles may hamper the productivity of the team. Navigating security verification, temporary credentials or waiting for access can cause delays.
- Lack of Scalability: As the organisation grows so does the complexity in configuration which needs regular checkups and improved provisions.
- Inconsistency: Misconfiguration can be a possible result of lack in standardisation of how systems are set up which may involve various administrators.

The solution lies in working closely with the hardware vendors to pre- load the operating systems with specific access and company templates before shipping of the devices. By reducing the dependencies on IT workers and minimizing manual usage, one touch provision welcomes a futuristic approach for customization and ultimately increasing productivity with decreased security issues.

III. Methodology: Zero Touch Provisioning Workflow

The architecture explains the comprehensive workflow for Microsoft Teams Room(MTR) through a Zero touch provision. It mainly talks about Automation, logistics and minimal manual usage.

A. Automation Workflow 1

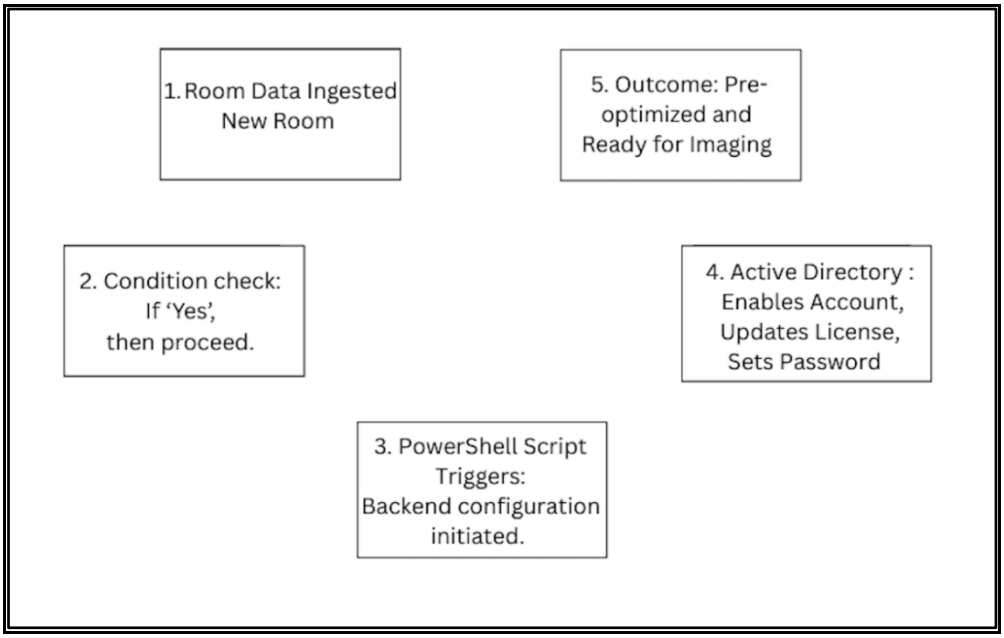

Fig. 1 Working of AW1: PowerShell driven Pre-provisioning process

- Creating the Resource Account

Once the room data is ingested and it surpasses the condition check as 'YES', a PowerShell is triggered by the workflow and a new resource account in the active directory is created. This account is not tied to personal use but by a system that bypasses user specific authentication such as two-factor authentication, enabling the system to login seamlessly and provides a smooth start. This multifaceted account does not belong to a sole user as a personal account rather it's ready to drive the moment anyone in the team needs it. No need for admin access for networks/ hardware or request any keys-it's pre-tuned to the job.

- Enable Account

- Assign Security group

- Assigning Permissions and Policies

The resource account is designated to the security groups via script and updates the enterprise specific metadata field accordingly:

- EA12 description update for fexin App

- EA2 Description update for CAP(Pro license)

- Set Standard Password

- Password never expire policy

These policies are mandatory as they define what the system can access and how it interacts with the other tools in the organisation. They have a ' never expire 'policy that ensures the meeting and automated room functions aren't due to unexpected password expiring.

- Giving access and starting system automatically

After the systematic orientation of account creation and policy assignments, the customized system is ready for use. Once the device is powered on, it connects to the network, Workspace ONE detects the serial number and matches it with the records in ServiceNow(SNOW). This setup checks the necessary details and forwards the specific credentials to the device. The system is now self aware of its working and now it does not require any manual intervention - it can login, configure and authenticate itself smoothly.

By blending the AD Integration, script-based configurations and device recognition, Automation Workflow 1 effectively lays the foundation for seamless zero touch experience. It efficiently turns provisioning into a background process. The system moves from a blank space to a pre-authorised, secure and ready to deploy devices, all before the manual use by the employees.

B. Automation Workflow 2

Succeeding the AW1, we have Automation Workflow 2, which talks about system preparation, license provisioning and post-deployment automation. This architecture ensures once the policy framework and account is set, the hardware identifies its particular identity, configurations and software without IT help.

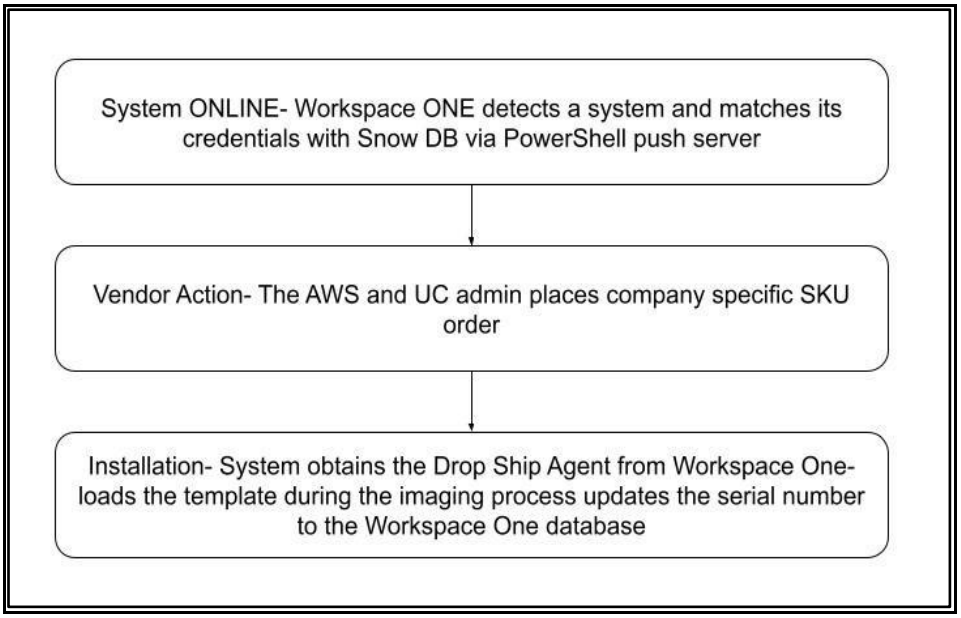

Fig. 2 Working of AW2: Device Provisioning, Imaging and License Activation

- Lenovo SKU Order

If a teams room is created and flagged in a system, a SKU unit order is placed to a vendor like Lenovo, Dell etc. SKU is customised as per organisation hardware and software requirement unlike the standard generic format.

- Predefined integration points for Workspace ONE
- Windows version and image type
- Specific Hardware Configuration (compute units, peripherals, etc)

SKU bridges the gap between Automation and Logistics. The vendor ensures that each SKU has every device shipped with the right drivers, firmware and provisioning hooks that need to form a customized system.

- Lenovo will add company data from Workspace ON

  As part of the above process, a Vendor Install Engineer initiates device imaging.

- A Drop Ship Agent is obtained from Workspace ONE
- The agent is installed to the system along with a pre-provisioned template.
- The device's serial number is then updated by the engineer to the Workspace ONE database

The Dropship Agent works as a lightweight software package which connects the system to Workspace ONE enabling:

- The system to optimise according to company specific configuration
- Validate system identity
- Starts post-provisioning steps automatically

Just after Automation Workflow 1, if the device states 'online' then the Workspace ONE detects the device and checks the database for serial number confirmation from ServiceNow (SNOW). Credential Assignment, License validation and Application setup is performed in each system for the company's use by the vendor. Separately, SNOW sends an automated request to MSIT, which assigns the required license. This facilitates the system to connect with Microsoft services and functions as a communication hub.

C. End to End Automation Architecture for Teams Room Deployment

The power of One Touch Provisioning lies in the continuous processing and closed loop system. Both Automation Workflow 1 and Automation Workflow 2 are key components of a broader provisioning pipeline. As soon as a device is brought for setup, a structured automation sequence is brought into action that builds a complete profile for that company's infrastructure. The resource account is established which is an enhanced version of personal account, where role based access is defined, metadata is used for licensing and system specific policies are applied- all without any manual intervention after depot.

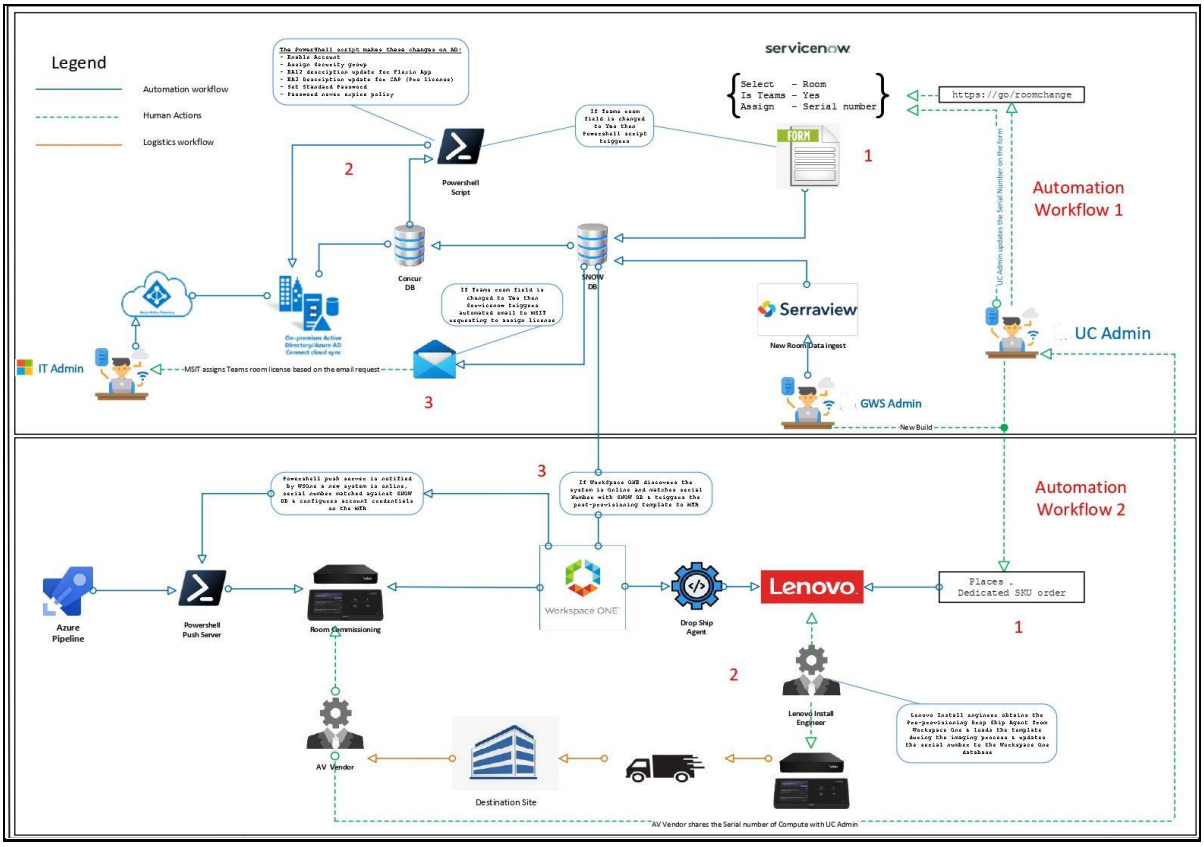

Fig. 3 MTR Zero Touch Provisioning Workflow

A virtual policy -bound representation of the system which is ready to be used and matches with the physical setup and application necessary for the company, acts as an essential part of stage one of provisioning. Once the system is processed and made ready at stage one it moves to the Workflow 2 that picks up a baton and ensures the alignment of the physical endpoint with its virtual counterpart. After coordinating with the hardware vendors, specific device configurations are selected and pre-imaged by tool. During this period the Dropship Agent binds the hardware to the resource account. As the device is turned on for final lookout, verification is performed via Workspace ONE- AV Vendor shares the Serial number of Compute with UC Admin.

The system's serial number is recognised thus it remembers its role, retrieves its licenses, activates performed configurations and services in real-time. It's a process that does not require any IT support. If AW1 sets the security parameters and policy then AW2 works hand in hand to incorporate physical instantiation of those policies. Together this Workflow act as a preemptive infrastructure service where users are not kept in waiting lists for signups rather the devices are born ready from the first instance. Ultimately the manual coordination among various teams, deployment time and risks associated with misconfiguration or data leak are reduced whether it's a large scale or small scale environment.

IV. TERMINOLOGIES

Powershell Push Server- This server acts as a Push mode which refers to a user actively applying a configuration to a target node by calling the Start Configuration. After creating and compiling a

configuration, one can enact it in push mode by calling the same, setting the -Path parameter of the cmdlet to the path where the configuration MOF is located. PowerShell Server is a server that makes remote system management and resource access easy.

- Dropship Agent- A dropshipping agent is a go-between for an organisation and its supplier. When you submit a sourcing request, the agent finds products from one or more suppliers based on what you need. The agent then purchases the items from the supplier(s) and takes care of quality checks, packaging, maybe even branding, and shipping straight to the customer.
- Workspace ONE - It's a digital workspace parameter developed with a unified endpoint that detects whenever a system is ONLINE, matches the credentials with records from the SnowDB and enables Dropship provisioning. It also ensures the license management, post- provisioning setup. It enables the company to deliver and manage any application on the device and virtual setup- through a single integrated platform.
- One Touch Provisioning(OTP)- This architecture explains how with a single touch the entire workflow can be handled at a time. The foundation of a complex back-end process starts with a single touch like it triggers a bullet and the entire setup gets into action with a pull.
- Resource Account- Unlike the usual personal account, this does not require any two- factor or multi-factor authentication. It has a variety of access and ID set into action before the initiation of a system. This is facilitated by the collaboration of the company and vendor for hardware and software optimization.
- Lenovo SKU- Stock Keeping Unit (SKU) is a company's imported tool for inventory management. It also has an unique alphanumeric code or identifier code that is put up on every device for its identification and use in future, sometimes it is also done via barcode for scanning and tracking the system in use.

V. Result and Future Scope

AW1 and AW2 as mentioned in fig. 3 demonstrates how significantly it can improve system efficiency, security posture and deployments.

- Reduced Human Errors: The chances of misconfiguration, forgotten access permissions are lowered by automation credential creation, licensing framework and group assignment.
- Improved Security and Compliance: Resource Account used here eradicates unnecessary user- level authentication, while still being governed by the organisational policy. Each device is traceable and compliant from the first instance.
- Optimised Vendor Collaboration - By working with the vendors at an early level through Dropship Agents and SKU ordering, the provision becomes an end-to-end setup ready for deployment.
- Operational Efficiency - Pre- configured software and credentials updated before deployment helps the timespan from several hours to minutes. No manual intervention or coordination among various teams is required by this architecture.

The key enhancements that can be implemented in future to this architecture are Dynamic Policy Application, cross-vendor expansion, integration with endpoint analytics, self-healing optimisation etc.

Challenges that can be faced during this working include configuration drift, dependency on network connectivity, single vendor lock-in risks etc.

Expanding the optimization to different vendors can increase the varieties in ideology and decrease the reliance on a single vendor, creating a dashboard for consistent status and alert checking can help improve the transparency and reduce the response timeframe. Introduction of new policies which adapt the geography and team role can help the system customisation and behaviour without IT intervention.

VI. CONCLUSIONS

This framework has helped the employees in an optimum way. It explores how the Zero Touch Provisioning, has involved building the synergy between two key aspects- Automation Workflow 1 and Automation Workflow 2, it executes the modern system deployment procedure and transforms the traditional approach to get a better outcome.

By the prerequisite of the digital ID or identity and incorporating this into a physical hardware infrastructure via vendor coordination and post provisioning methodology, big organisations are not just building a future for their workers but also optimising the IT sector in an efficient way.

The construction discussed in this research paper not only talks about reduced manual usage but also it helps the organisation work smoothly during system handover to its employees. It improves security, creates suditable and intelligent provisioning pipeline. Enhancing the overall onboarding experience, improves global impact- this is what the setup here aims for. It basically acts as a launchpad for next gen IT management - where empowering the system from the beginning is what helps everything to fall into place and align in a systematic line.

REFERENCES

1. michaeltlombardi, “Enacting configurations - PowerShell,” Microsoft.com, Dec. 13, 2021. https://learn.microsoft.com/en-us/powershell/dsc/pull-server/enactingconfigurations?view=dsc-1.1
2. “/n software,” Nsoftware.com, 2025. https://www.nsoftware.com/powershellserver
3. | AnhNN-CTV, “Dropshipping Agent: A Comprehensive Guide In 2025,” SimiCart Blog | Empowering Ecommerce Growth with Mobile Solutions since 2011, Oct. 24, 2024. https://simicart.com/blog/dropshipping-agent/
4. mkbond007, “Manage resource accounts for service numbers - Microsoft Teams,” Microsoft.com, Apr. 10, 2025. https://learn.microsoft.com/en-us/microsoftteams/manage-resource-accounts
5. “About administrator roles - Google Workspace Admin Help,” Google.com, 2019. https://support.google.com/a/answer/33325?hl=en
6. Wikipedia Contributors, “Stock keeping unit,” Wikipedia, Nov. 07, 2019. https://en.wikipedia.org/wiki/Stock_keeping_uni