**Type of Service Now Users**

End Users

* Has no roles and is typically in non-IT

Power Users

* Has ITIL role and is in IT

System Administrator

* Has Admin rights to the SNOW platform.

Contact Types in SNOW for End User.

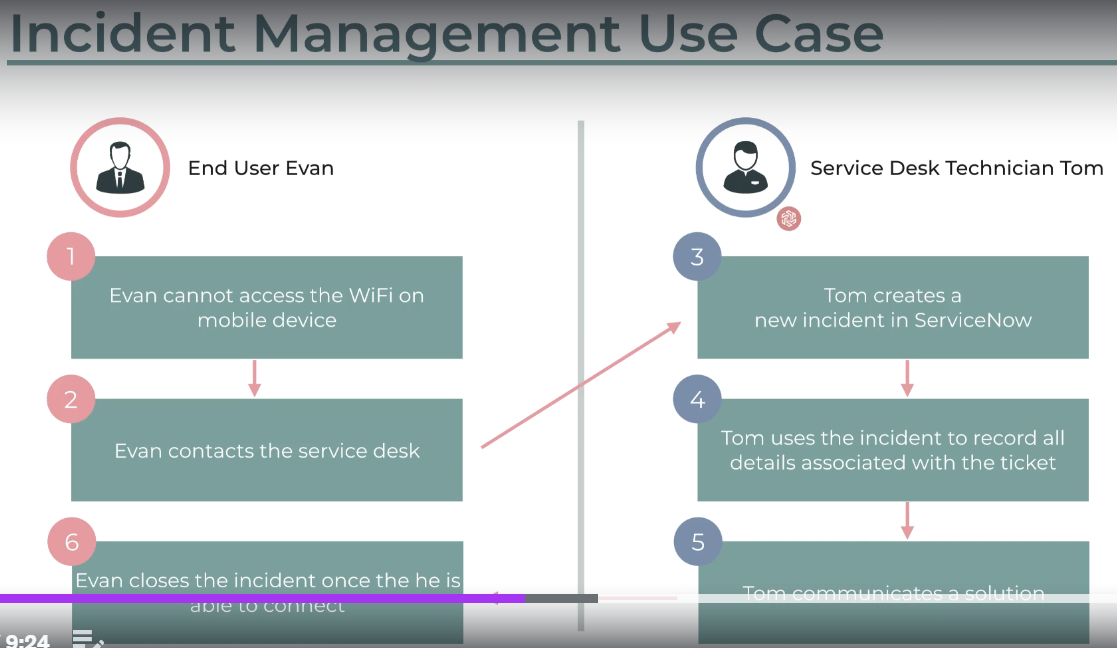
* SNOW End-user view/service portal view
* Call at IT helpdesk number
* Chat
* Email

Contact Types in SNOW for Service Desk (Power User)

* Platform View of SNOW

**Incident management**

Incident management is a formal process used to identify, diagnose, and resolve **unexpected disruptions** to IT services or business operations. It's essentially a structured approach to getting things back to normal as quickly as possible when something goes wrong.



**Service Desk Technician: Resolving End User WiFi Issue**

**Scenario:** An end user, Sarah Lee, reports an inability to connect to the company WiFi network.

**End User Actions:**

1. Sarah contacts the IT service desk through a preferred channel (phone, email, self-service portal).
2. She describes the issue, including any error messages or troubleshooting attempts.

**Service Desk Technician Actions:**

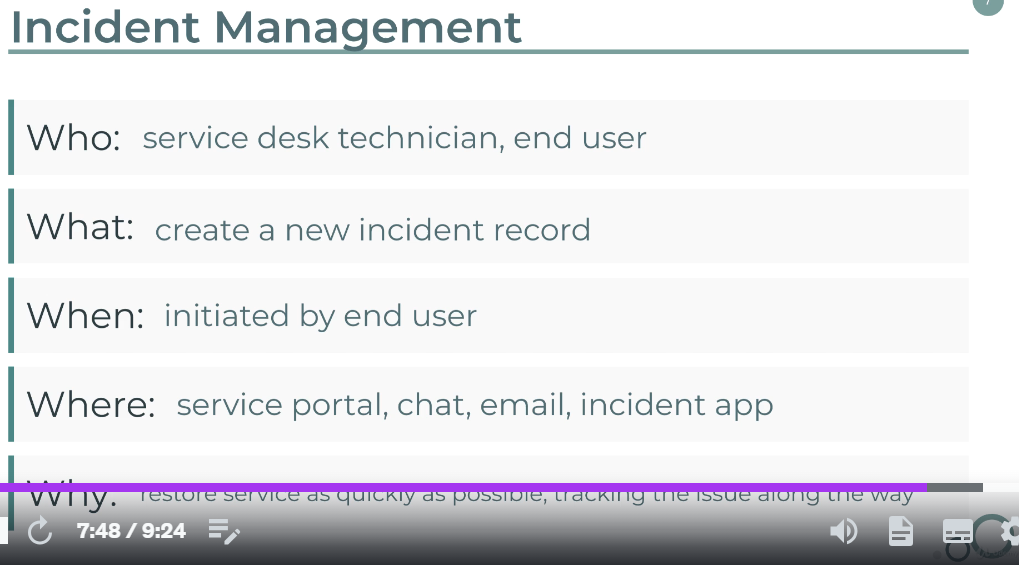
1. **Gather Information:** The technician asks clarifying questions to understand the problem better. These might include:
   * Device type (laptop, phone, etc.)
   * Specific error messages encountered (if any)
   * Recent changes to the device or network settings
   * Troubleshooting steps already taken
2. **Initial Diagnosis:** Based on the gathered information, the technician attempts a basic diagnosis:
   * **Knowledge Base Search:** They check for existing solutions or troubleshooting guides in the company's knowledge base.
   * **Account Verification:** They verify if Sarah's device is registered on the network.
3. **Resolution:** Depending on the diagnosis, the technician takes these steps:
   * **Simple Solution:** If the issue is user-specific and easily resolved (e.g., forgetting/reconnecting to the WiFi), the technician guides Sarah through the steps.
   * **Remote Assistance:** With Sarah's permission, the technician may remotely access her device to adjust settings or troubleshoot further.
   * **Escalation:** If the issue is beyond their expertise or requires network changes, the technician escalates the ticket to the appropriate team (e.g., network operations).
4. **Communication:** Throughout the process, the technician keeps Sarah updated via the chosen communication channel (phone call, email updates within the ticket system, etc.).

**Resolution and Follow-up:**

* **Successful Resolution:** If the technician resolves the issue, they document the solution in the ticket for future reference. Sarah receives confirmation that the issue is fixed.
* **Escalation:** If the issue requires further investigation, the technician clarifies the next steps with Sarah, including an estimated timeframe for resolution.

**Benefits of a Service Desk System:**

* **Streamlined Process:** The system guides technicians through a consistent workflow, ensuring efficient issue resolution.
* **Centralized Communication:** All communication is documented within the ticket, improving visibility and collaboration.
* **Improved User Experience:** Clear updates keep Sarah informed of the progress, fostering a positive support experience.



Incident management deals with unplanned events that disrupt IT services or business operations. Here are some ways to categorize these incidents:

**By Impact:**

* **High Impact:** These incidents cause significant disruption to critical business functions or services, affecting a large number of users. Examples include:
  + Major system outage
  + Widespread network failure
  + Data loss event
* **Medium Impact:** These incidents disrupt some business functions or services, impacting a moderate number of users. Examples include:
  + Application slowdown
  + Printer malfunction affecting a department
  + Denial-of-service attack (DoS) causing temporary disruption
* **Low Impact:** These incidents cause minor disruptions to individual users or have minimal impact on business operations. Examples include:
  + Password reset request
  + Individual software malfunction
  + Minor website glitch

**By Urgency:**

* **Critical:** These incidents require immediate attention to prevent significant loss or damage. Examples include:
  + Security breach
  + Data loss event requiring immediate action
  + System outage impacting emergency services
* **High:** These incidents require prompt attention to minimize downtime or disruption. Examples include:
  + Major application error causing widespread issues
  + Critical system performance issue impacting core operations
* **Medium:** These incidents can be addressed within a reasonable timeframe. Examples include:
  + Minor application error affecting a small group
  + Non-critical system performance issue

**By Type of Service Affected:**

* **Hardware:** Issues related to physical devices like servers, printers, or workstations. Examples include:
  + Hardware failure causing a system outage
  + Printer malfunction halting printing operations
  + Overheated server causing performance issues
* **Software:** Problems with applications, operating systems, or other software programs. Examples include:
  + Software bug causing application crashes
  + Operating system update causing compatibility issues
  + Security vulnerability in a critical application
* **Network:** Connectivity issues, network outages, or performance problems. Examples include:
  + Internet outage affecting all users
  + Network congestion slowing down operations
  + Denial-of-service attack (DoS) targeting network resources
* **Security:** Suspicious activity, security breaches, or unauthorized access attempts. Examples include:
  + Phishing attack targeting employees
  + Malware infection compromising user data
  + Unauthorized access attempt to a critical system

MIR, or Major Incident Response, refers to a specific process within incident management that deals with high-impact events that significantly disrupt IT services or business operations. It's essentially an escalation plan for handling critical situations. Here's a breakdown of MIR:

**Purpose:**

* To ensure a swift and coordinated response to major incidents that threaten critical business functions.
* To minimize downtime, data loss, and financial impact associated with such incidents.

**Characteristics:**

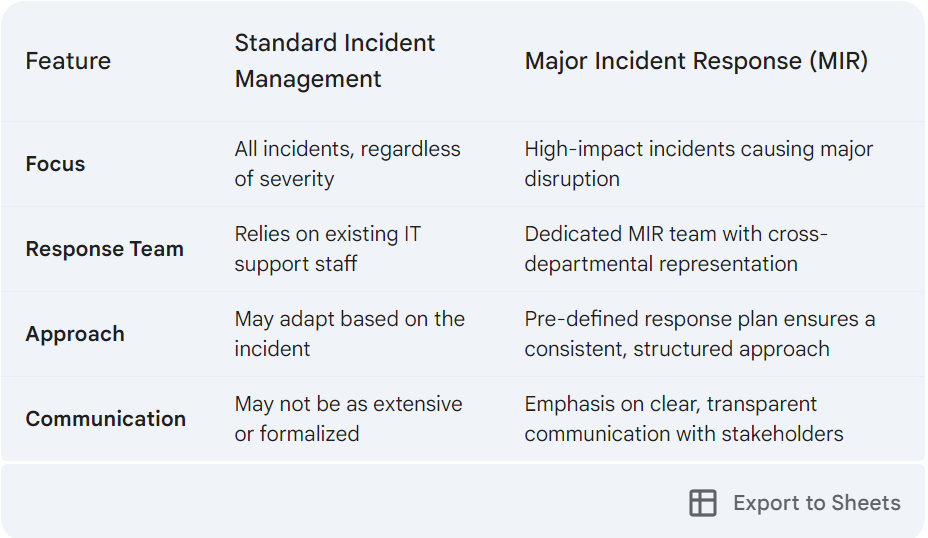
* **High Impact:** Focused on incidents that cause widespread disruption or pose a significant risk to the organization. (e.g., Major system outage impacting all users, critical data breach)
* **Dedicated Team:** Often involves forming a dedicated Major Incident Response (MIR) team with representatives from various departments (IT, security, operations, management) to collaborate on resolving the issue.
* **Structured Approach:** Utilizes a pre-defined response plan outlining roles, responsibilities, communication protocols, and escalation procedures.
* **Communication & Transparency:** Effective communication with stakeholders, keeping everyone informed about the incident, progress, and estimated recovery time.

**Benefits:**

* **Faster Resolution:** Dedicated team and structured approach lead to quicker identification and resolution of major incidents.
* **Reduced Impact:** Minimizes downtime, data loss, and financial damages by responding swiftly and efficiently.
* **Improved Recovery:** Facilitates a smooth recovery process and helps get things back to normal as quickly as possible.

**Comparison with Standard Incident Management:**

While standard incident management handles all disruptions, MIR focuses specifically on critical events. Here's a table summarizing the key differences:



1. **Standard Changes:**

* **Description:** Pre-approved, low-impact, routine changes with well-defined procedures and minimal risk. Examples include adding a new user account, updating standard software versions, or replacing a failing hard drive with an identical model.
* **Process:** Often have a streamlined approval process or may even be pre-approved based on pre-defined criteria.

1. **Normal Changes:**

* **Description:** Planned changes that require a formal change request process with impact assessment and approval. These changes may have some degree of risk or require more resources compared to standard changes. Examples include installing a new software application, migrating data to a new server, or modifying network configurations.
* **Process:** Follow a defined change management workflow involving impact assessment, risk evaluation, approval by relevant stakeholders, and potentially a testing phase before deployment.

1. **Emergency Changes:**

* **Description:** Urgent changes required to address critical situations that pose a significant security risk or disruption to operations if left unaddressed. Examples include patching a critical security vulnerability, restoring a critical system outage, or taking action during a security breach.
* **Process:** Expedited approval process with limited review due to urgency. May involve higher risk due to the lack of extensive testing or impact assessment. A thorough review is still conducted after the situation stabilizes to assess effectiveness and identify lingering risks.

In addition to these main categories, some organizations might also use:

* **Major Changes:** These are significant changes with potentially high impact or risk, requiring a more comprehensive review and approval process compared to normal changes. Examples include implementing a new enterprise resource planning (ERP) system or migrating to a cloud environment.

The specific types of change requests and their categorization might vary depending on the organization's size, structure, and risk tolerance.

**Change management**

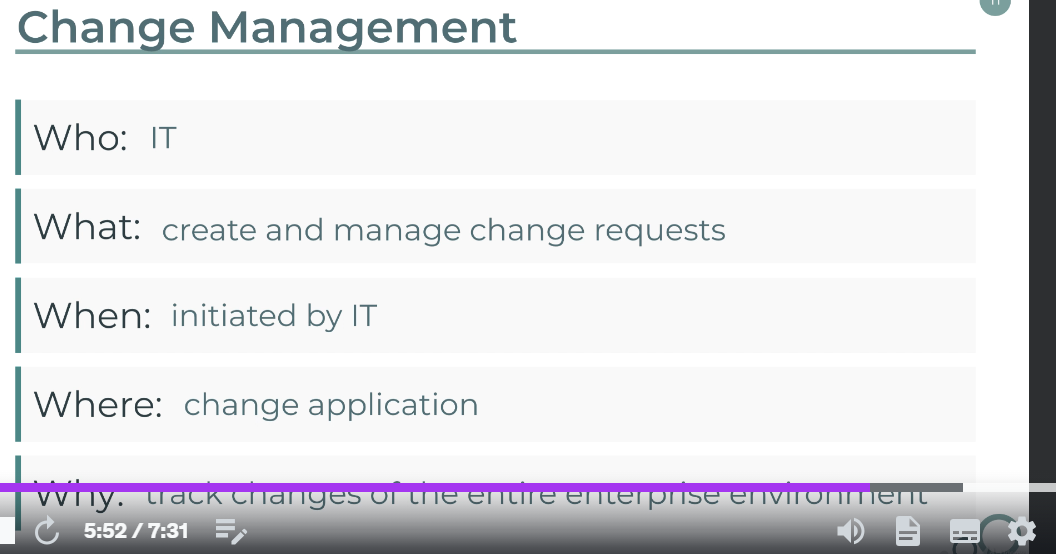
IT change management is a systematic approach **to planning, implementing, and reviewing modifications to IT infrastructure**, systems, applications, or processes. Its primary goal is to minimize disruption and risk while ensuring the successful implementation of changes.

Typically involves a defined workflow with stages like:

* **Change Request:** A formal proposal outlining the change, its purpose, and potential impact.
* **Impact Assessment:** Evaluation of potential risks and disruptions associated with the change.
* **Approval Process:** Review and authorization by relevant stakeholders based on the impact assessment.
* **Implementation & Testing:** Careful execution of the change with thorough testing to ensure functionality.
* **Deployment & Monitoring:** Deployment of the change to production and close monitoring for any issues.
* **Closure:** Documentation of the change process, lessons learned, and post-implementation review.

Example

Upgrading a company's customer relationship management (CRM) system.

1. **Change Request:** The IT department submits a request to upgrade the CRM system to a newer version with improved features.
2. **Impact Assessment:** The team analyzes the potential impact, including downtime for data migration and user training needs.
3. **Approval Process:** The request is reviewed by management, considering the impact and potential benefits.
4. **Implementation & Testing:** The IT team installs the new CRM system in a test environment, thoroughly testing functionality and data migration.
5. **Deployment & Monitoring:** The new CRM system is deployed to the production environment during a scheduled maintenance window. IT monitors for any issues and user adoption.
6. **Closure:** The change management process is documented, including lessons learned from testing and deployment. User feedback is collected for further improvements.
7. ------------------------------------------------------------------------------------------------------------
8. 

**Configuration Management**

Configuration management (CM) is the process of establishing and maintaining consistency in a system's attributes throughout its lifecycle. In simpler terms, it's about ensuring all the components of a system, like hardware, software, and settings, are set up and remain in the desired state.

Here's a breakdown of what CM involves:

* **Establishing a Baseline:** Defining the desired configuration for each element of the system. This includes hardware settings, software versions, security configurations, and any other relevant details.
* **Tracking Changes:** Monitoring and documenting any modifications made to the system's configuration. This ensures a clear history of changes and allows for reverting to previous states if necessary.
* **Maintaining Consistency:** Verifying that all components of the system adhere to the established baseline configuration. This helps prevent inconsistencies that might lead to malfunctions or security vulnerabilities.
* **Version Control:** Tracking different versions of the system configuration, allowing for rollbacks if issues arise after updates.

**Benefits of Configuration Management:**

* **Reduced Downtime:** By maintaining consistent configurations, CM helps prevent unexpected issues and minimizes downtime caused by inconsistencies.
* **Improved Security:** Consistent security configurations across the system minimize vulnerabilities and improve overall security posture.
* **Simplified Troubleshooting:** Documented configurations facilitate faster troubleshooting by providing a clear picture of the system's setup.
* **Enhanced Compliance:** CM helps ensure systems comply with internal policies and external regulations.
* **Improved Automation:** Standardized configurations enable automation of deployment and configuration management tasks, saving time and resources.

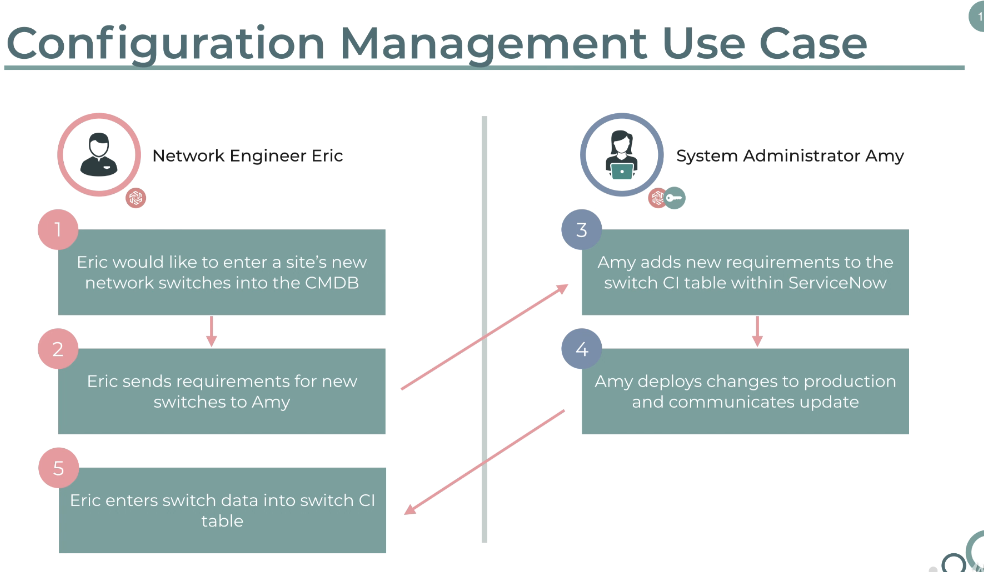
**Applications of Configuration Management:**

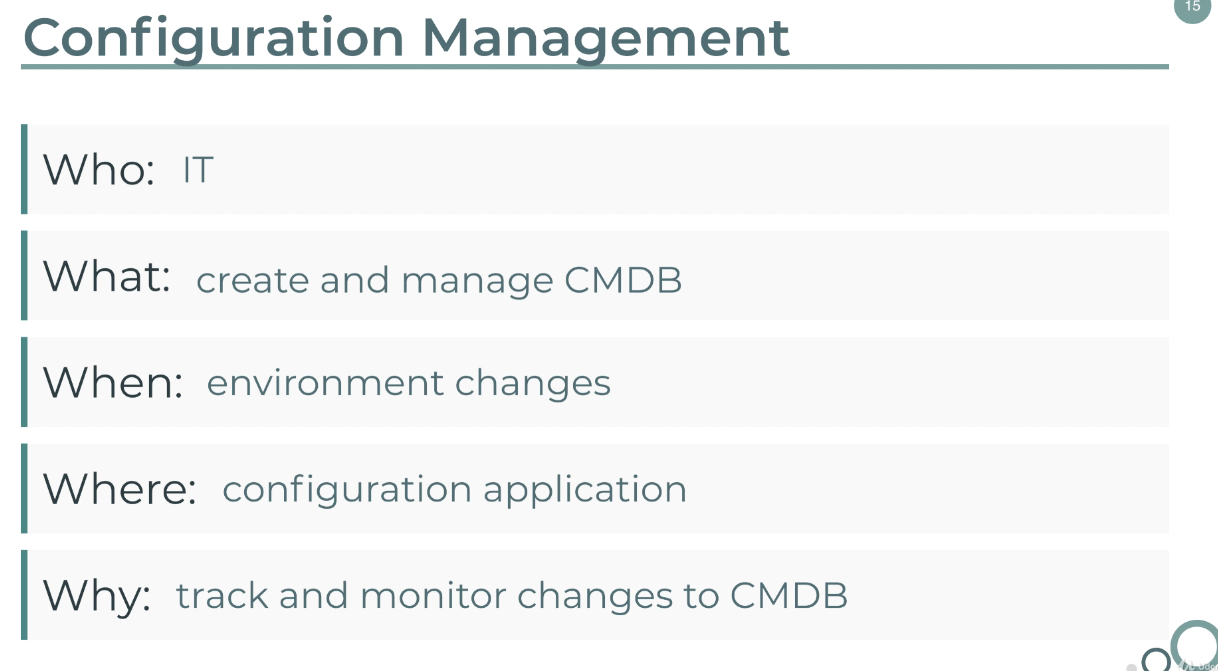
* **IT Infrastructure:** Managing configurations of servers, network devices, and other IT equipment.
* **Software Development:** Ensuring consistent configurations across development, testing, and production environments.
* **Security Management:** Maintaining consistent security configurations across all systems and devices.
* **Cloud Computing:** Managing configurations of virtual machines and cloud resources.

**Popular Configuration Management Tools:**

* Ansible
* Chef
* Puppet
* SaltStack

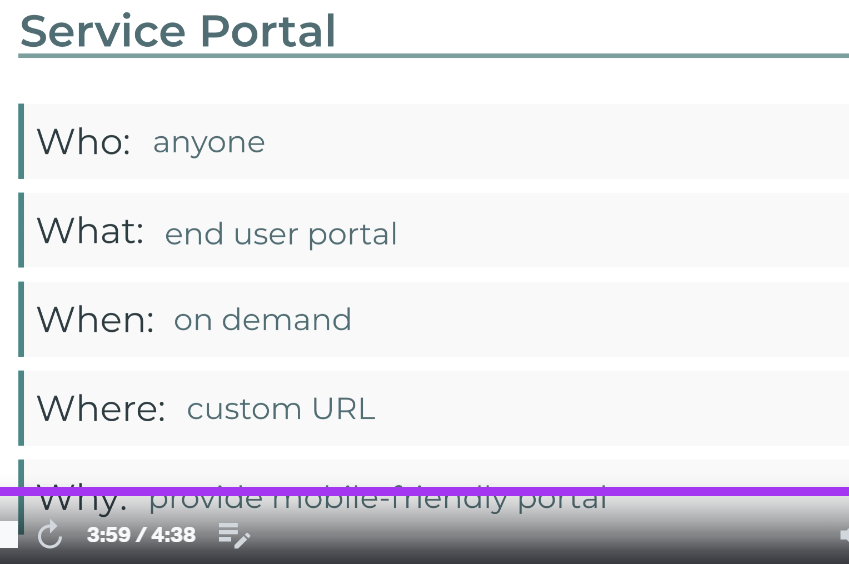
By implementing configuration management practices, organizations can ensure their systems are reliable, secure, and easier to manage, ultimately improving overall efficiency and reducing risks.

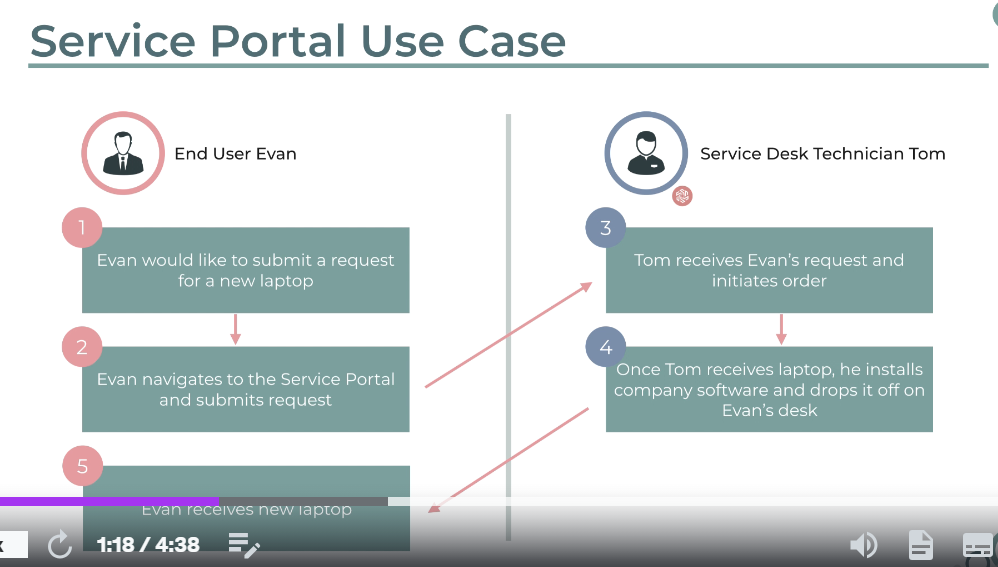




Service Portal

Service Portal in ServiceNow (SNOW) is a web-based interface that allows end-users (employees, customers, etc.) to self-service their IT needs. It acts as a single point of access for various IT services, resources, and functionalities.





**Snow Tutorial**

Creating Incident

Creating Problem

Creating Knowledge article