NM1051—SERVICENOW ADMINISTRATOR

OPTIMIZING USER GROUP AND ROLE MANAGEMENT WITH ACCESS CONTROL AND WORKFLOWS

A PROJECT REPORT

Submitted By

MALATHI.E	**–**	**961322104025**
GAYATHRI DEVI .E	**-**	**961322104017**
AJAY P.J	**-**	**961322104005**
BHARATHI KANNAN .S	**-**	**961322104010**

BACHELOR OF ENGINEERING

IN SEVENTH SEMESTER

COMPUTER SCIENCE ENGINEERING

M.E.T ENGINEERING COLLEGE , AARALVAAIMOZHI- 629301

ANNA UNIVERSITY: CHENNAI 600025 /DECEMBER -20

ACKNOWLEDGEMENT

I am deeply grateful to express my sincere thanks to M.E.T Engineering college, for providing me the opportunity to undertake this project **titled** “ServiceNow Project Management and Role-Based Access Control System.”

I would like to extend my heartfelt gratitude to our Principal, and Head of the Department, for their continuous encouragement, support, and for providing all the necessary facilities to carry out this project successfully.

My sincere thanks to my project guide,for their valuable guidance, patience, and constant motivation throughout the project. Their expert advice and constructive feedback have been instrumental in shaping this work.

I also extend my appreciation to all the faculty members **of the** Department of Computer Science and Engineering for their support and valuable suggestions during the various stages of this project.

A special thanks to my friends and classmates for their continuous encouragement, valuable insights, and cooperation throughout the completion of this project.

Finally, I express my deepest gratitude to my family members for their unwavering love, moral support, and understanding during the entire duration of this work.

S. No.	Content	Page No.
1.	**ABSTRACT**	4
2.	**INTRODUCTION**	5
3.	**OBJECTIVES**	6
4.	**METHODOLOGY**	7
5.	**EXISTING SYSTEM AND DRAWBACKS**	8
6.	**PROPOSED WORK**	9
7	**SYSTEM REQUIREMENTS**	10
6.1	Hardware Requirements	10
6.2	Software Requirements	10
8.	**MODULES DESCRIPTION**	11
9.	**SYSTEM DESIGN:**	12
10.	**WORKFLOW DESCRIPTION:**	13
11.	**DATA FLOW DIAGRAM:**	14
12.	**IMPLEMENTATION**	15
13.	**ACCESS CONTROL CONFIGURATION :**	26
14.	**USER ROLES AND PERMISSIONS MATRIX**	27
15.	**TESTING**	28
16.	**RESULTS AND DISCUSSION**	29
17.	**ADVANTAGES**	30
18.	**APPLICATIONS**	31
19.	**FUTURE ENHANCEMENTS**	32
20.	**CONCLUSION**	33
21.	**BIBLIOGRAPHY**	34

ABSTRACT:

The project titled "Optimizing User, Group, and Role Management with Access Control and Workflows" is developed on the ServiceNow platform to streamline and automate the management of users, groups, and roles within an organization. The objective of this project is to design an efficient, secure, and scalable system that minimizes manual administrative tasks, enhances transparency, and ensures proper access control to organizational resources.

In many IT environments, managing user accounts and access privileges manually can lead to inconsistencies, security vulnerabilities, and delays in task execution. To address these challenges, this project leverages ServiceNow's workflow automation capabilities**,** Access Control Lists (ACLs)**,** and Flow Designer to create a dynamic and policy-driven user management framework. Automated workflows handle user creation, role assignment, and approval requests, thereby reducing human dependency and ensuring faster response times.

The system empowers administrators and project managers to efficiently manage user profiles, assign roles based on responsibilities, and monitor project-related activities while maintaining strict data security. Using ACLs, sensitive operations and data are protected by role-based restrictions, ensuring that only authorized users can perform specific actions. Additionally, the use of Flow Designer automates approval processes and task generation, increasing overall operational efficiency and accountability.

This project highlights the critical role **of** role-based security**,** workflow automation, and access governance in modern IT Service Management (ITSM) systems. By integrating these features within the ServiceNow platform, the proposed solution not only simplifies administrative tasks but also contributes to improved compliance, productivity, and user experience across the organizations

1.INTRODUCTION

In modern organizations, managing users, roles, and access permissions efficiently has become a critical aspect of IT service management. As enterprises continue to adopt digital platforms, ensuring that the right individuals have appropriate access to systems and data is essential for maintaining security, compliance, and operational efficiency. Manual management of user accounts, group memberships, and access rights often leads to inconsistencies, security vulnerabilities, and administrative delays. To address these challenges, this project, “Optimizing User, Group, and Role Management with Access Control and Workflows,” has been developed using the ServiceNow platform.

ServiceNow is a cloud-based IT Service Management (ITSM) tool that provides a centralized framework for automating workflows, managing incidents, and maintaining access controls. The proposed system focuses on automating the creation, modification, and approval processes for users and roles within an organization. By leveraging ServiceNow’s Access Control Lists (ACLs)**,** Flow Designer**,** and Workflow automation features**,** the project establishes a secure, rule-based environment where administrative tasks can be executed efficiently with minimal human intervention.

The system introduces structured modules for user account management**,** role assignment**,** group management**,** and workflow-based approvals**.** Each module interacts seamlessly to maintain data integrity, ensure accountability, and streamline task management. Managers and administrators can easily assign roles, approve access requests, and monitor changes, while the system automatically enforces access control rules to prevent unauthorized activities.

Through this project, organizations can achieve enhanced transparency, security, and efficiency in managing their IT operations. It reduces manual workload, eliminates redundant processes, and ensures that access privileges are aligned with organizational policies. The use of ServiceNow’s automation tools demonstrates the power of low-code development platforms in building scalable enterprise solutions.

In summary, this project serves as a practical implementation of role-based access control (RBAC) and workflow automation principles in a real-world environment. It highlights how ServiceNow can be effectively used to enhance IT governance, improve productivity, and ensure secure user management across the organizational ecosystem.

2.PROBLEM STATEMENT

In modern organizations, managing users, groups, and roles has become a complex and time-consuming process due to the increasing number of employees, departments, and digital systems. Manual methods of creating, updating, and managing user accounts often result in inconsistencies, security risks, and operational inefficiencies. When user access is not properly controlled, it can lead to unauthorized access to confidential data, violation of compliance policies, and a lack of accountability within the system. These challenges highlight the urgent need for a secure and automated approach to handle user lifecycle management effectively.

Traditionally, administrators manually assign roles and manage user permissions, which increases the risk of human error and delays in task approvals. For instance, when a new employee joins an organization, creating an account, assigning the appropriate role, and providing access to the necessary resources can take a considerable amount of time. Similarly, when employees leave or change departments, their access rights must be promptly updated or revoked to prevent misuse of system resources. Without automation, these tasks often get overlooked or delayed, causing data security issues and inefficiencies in workflow management.

Furthermore, many organizations lack a centralized system that tracks and manages user roles, group memberships, and access privileges. The absence of integrated workflows makes it difficult for administrators to monitor approvals, manage tasks, and ensure compliance with internal policies. This manual dependency not only reduces productivity but also increases the risk of unauthorized access and data breaches.

To overcome these challenges, there is a clear need for a system that automates user and role management processes while maintaining strict access controls. The system should allow administrators to manage users, assign roles, and monitor activities efficiently through a centralized platform. It should also include automated approval workflows and Access Control Lists (ACLs) to ensure only authorized users can perform sensitive actions. Implementing such a solution on the **ServiceNow platform** can significantly enhance operational efficiency, reduce human error, and ensure secure, transparent, and policy-compliant access management across the organization.

3.OBJECTIVES:

1. Automated and secure system:

The primary objective of this project is to design and implement an automated and secure system for managing users, groups, and roles within an organization using the ServiceNow platform. The system aims to reduce manual interventions, enhance data security, and improve overall operational efficiency through workflow automation and access control mechanisms. By integrating role-based permissions and approval processes, the project ensures that every user action within the system is authorized, traceable, and policy compliant.

2. Automate user lifecycle management

One of the main objectives is to automate user lifecycle management, including account creation, role assignment, and access modification. This eliminates repetitive manual processes and ensures that users are granted appropriate permissions based on their job responsibilities. Another key objective is to implement Access Control Lists (ACLs) to restrict unauthorized access to sensitive data and functionalities, thereby maintaining system integrity and confidentiality.

3. Utilize ServiceNow Flow Designer

The project also aims to utilize ServiceNow Flow Designer to create automated workflows for approval and task management. This feature helps streamline operations such as user onboarding, role change approvals, and task assignments, ensuring that each process follows a predefined and auditable sequence. Through these workflows, administrators and managers can monitor and approve requests efficiently, reducing delays and human errors.

4. Provide a centralized management dashboard

In addition, the system intends to provide a centralized management dashboard that offers administrators a unified view of all users, groups, and their assigned roles. This centralized approach simplifies monitoring, reporting, and auditing, thereby improving transparency and accountability across the organization.

5. Enhance security and compliance

Another important objective is to enhance security and compliance by ensuring that all access privileges are aligned with organizational policies. This includes enforcing role-based access control (RBAC) and maintaining logs of all user actions for future audits.

6. demonstrate the importance of workflow automation and access governance

Ultimately, the project aims to demonstrate the importance of workflow automation and access governance in modern IT Service Management (ITSM). By leveraging the capabilities of the ServiceNow platform, the system will serve as a scalable, secure, and efficient model for managing users, roles, and workflows in any enterprise environment.

4. Methodology :

1.Systematic And Structured Approach:

The methodology adopted for this project is a systematic and structured approach to ensure the successful development and implementation of a secure and automated user, group, and role management system using the ServiceNow platform. The project follows a combination of the Waterfall model and Agile principles, ensuring both step-by-step execution and flexibility in system enhancements.

2. **Requirement Analysis**,

The development process begins with requirement analysis, where the functional and non-functional requirements of the system are identified. This stage involves understanding organizational needs related to user account management, access control, and workflow automation. The analysis also includes identifying the limitations of the existing manual system and determining how automation can enhance operational efficiency.

3. System Design

The second stage focuses on system design, where the architecture, data models, and access control structures are defined. ServiceNow's built-in modules, such as User Tables, Roles, Groups, and Access Control Lists (ACLs), are customized to meet the project's requirements. The Flow Designer tool is used to automate approval and task creation workflows, ensuring that every request passes through proper authorization channels before execution.

4. **Implementation And Configuration**,

The third stage involves implementation and configuration, where the designed workflows, tables, and ACLs are developed and integrated within the ServiceNow environment. Custom forms, UI policies, and business rules are created to enhance user interaction and data validation. During this phase, various user roles—such as Administrator, Project Manager, and Team Member—are configured with specific permissions to ensure a secure environment.

5. **Testing And Validation**,

The fourth stage includes testing and validation, where the system undergoes functional, integration, and user acceptance testing. Each module is tested to ensure that workflows execute correctly, access permissions are properly enforced, and data integrity is maintained.

6.Deployment And Evaluation

Finally, the deployment and evaluation phase ensures the system is successfully implemented in a live environment. Feedback from administrators and users is collected to identify any potential improvements.

5. EXISTING SYSTEM AND DRAWBACKS

In most organizations, the existing system for managing users, groups, and roles is largely **manual or semi-automated**, relying heavily on administrative personnel to create, modify, and deactivate user accounts. The management of access privileges and approval processes is often handled through spreadsheets, emails, or standalone tools that are not integrated into a centralized platform. This manual approach is not only time-consuming but also prone to human errors and inconsistencies.

Typically, when a new employee joins an organization, system administrators must manually create a user account, assign appropriate roles, and provide access to various modules or applications. Similarly, when employees transfer between departments or leave the company, administrators must manually update or revoke their access. In large organizations with hundreds or thousands of employees, these repetitive tasks consume significant time and resources. Moreover, without proper automation, there is often no systematic tracking or audit trail for user access and role changes, making it difficult to ensure compliance with organizational security policies.

Another major drawback of the existing system is **the** lack of automated workflows for approvals and task management. When role changes or new access requests are made, approvals are usually sought via emails or informal communication channels, which can lead to delays, lost requests, or unauthorized approvals. This not only reduces operational efficiency but also increases the risk of unauthorized access to sensitive information.

Additionally, traditional systems often lack role-based access control (RBAC**)** and Access Control Lists (ACLs)**,** which are critical for ensuring data confidentiality and integrity. Without these controls, users may gain access to information or functions beyond their job responsibilities, posing serious security threats. The absence of centralized monitoring and reporting tools further limits administrators’ ability to analyze user activities and detect policy violations.

In summary, the existing system suffers from inefficiency, lack of transparency, and poor security enforcement. The absence of automation leads to delayed approvals, human errors, and compliance challenges. These drawbacks emphasize the need for a **modern, automated, and secure solution**—one that integrates user management, access control, and workflow automation within a unified platform such as **ServiceNow** to enhance productivity, accountability, and security across the organization.

6. PROPOSED SYSTEM

.

The proposed system, titled **“Optimizing User, Group, and Role Management with Access Control and Workflows,”** introduces an automated, secure, and centralized solution built on the **ServiceNow platform**. It is designed to overcome the limitations of the traditional manual system by integrating workflow automation, access control, and role-based management into a single, efficient platform. The system leverages ServiceNow’s powerful tools—**Flow Designer**, **Access Control Lists (ACLs)**, and **custom application modules**—to streamline user management operations and ensure data security.

In the proposed system, administrators can create, update, and manage user accounts seamlessly. When a new user is added, the system automatically assigns them to a specific group and role based on their job responsibilities. The approval process for new user accounts and role modifications is handled automatically through ServiceNow’s **Flow Designer**, eliminating the need for manual interventions. This automation not only reduces administrative workload but also minimizes human error and ensures faster processing of requests.

The use of **Access Control Lists (ACLs)** adds an extra layer of security by defining which users have permission to access or modify certain records, modules, or data. This ensures that sensitive information is only accessible to authorized personnel, maintaining confidentiality and compliance with organizational policies. Role-based access control (RBAC) ensures that users have access privileges strictly aligned with their assigned responsibilities, preventing unauthorized actions.

Additionally, the proposed system provides a **centralized dashboard** where administrators can view and manage all user accounts, groups, and workflows in real time. Managers can easily approve or reject access requests through automated notifications, improving communication and transparency. The system also maintains detailed audit trails of all user actions, enabling better accountability and easier tracking during security audits.

By integrating automation and access control within the ServiceNow environment, the proposed system significantly improves efficiency, accuracy, and data security. It transforms the user management process into a structured and policy-driven workflow that aligns with modern IT Service Management (ITSM) standards. Ultimately, this system enhances operational performance, ensures compliance, and provides a scalable foundation for future organizational growth.

7. SYSTEM REQUIREMENTS

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” is developed on the ServiceNow cloud platform, which requires minimal hardware and software resources. Since ServiceNow operates as a Software as a Service (SaaS) model, all data storage, workflow automation, and processing are handled on the cloud.

Hardware Requirements:

A standard computer or laptop with at least an **Intel Core i3 processor**, **4 GB RAM (8 GB recommended)**, and **stable internet connectivity** is sufficient. A modern web browser such as **Google Chrome, Mozilla Firefox, or Microsoft Edge** is required for accessing the platform.

Software Requirements:

The project uses only the **ServiceNow platform** and its built-in tools such as **Flow Designer**, **Access Control Lists (ACLs)**, **Form Designer**, and **Table Builder**. No external software or local server setup is needed, making the system lightweight, cost-effective, and easy to maintain.

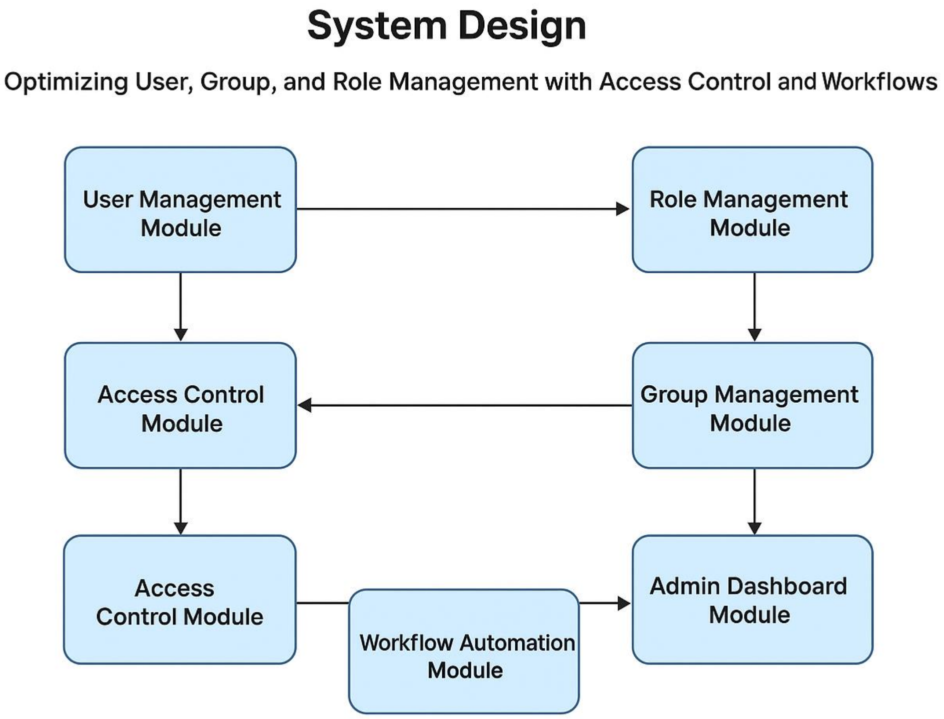
8. MODULES DESCRIPTION

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” is divided into several key modules that work together to automate and secure user management within the ServiceNow platform. Each module performs a specific function to ensure smooth operation, controlled access, and workflow automation.

1. **User Management Module:**
   Handles the creation, updating, and deletion of user accounts. It automates assigning users to appropriate roles and groups based on their job responsibilities.
2. **Role Management Module:**
   Manages different user roles within the organization. It defines permissions and access levels to ensure that users can only perform authorized actions.
3. **Group Management Module:**
   Organizes users into groups for easier task assignment and project coordination. Administrators can manage team memberships efficiently.
4. **Access Control Module (ACL):**
   Ensures data security by restricting access to specific modules, tables, or records based on user roles.
5. **Workflow Automation Module:**
   Uses **Flow Designer** to automate approval processes and task creation, reducing manual work and human errors.
6. **Admin Dashboard Module:**
   Provides a centralized interface for administrators to monitor users, approvals, and workflows in real time.

9.SYSTEM DESIGN:

The system design includes user entities, role relationships, and workflows that govern approvals. The architecture ensures modularity and scalability, supporting future enhancements like HR integration.



10. WORKFLOW DESCRIPTION:

The workflow of the proposed ServiceNow project is designed to automate and streamline the process of user and project management within an organization. It provides a systematic flow from user account creation to approval, role assignment, and project access. The workflow ensures that every task follows a predefined sequence, reducing manual errors and improving transparency.

The process begins when a new user or project member requests access to the system. The workflow starts with the **User Account Creation** stage, where basic details such as name, email, and department are entered into the ServiceNow platform. Once the request is submitted, it automatically moves to the **Assign Roles** phase. In this stage, appropriate roles such as *Project Member*, *Team Member*, or *Project Manager* are assigned based on the user's designation or responsibility within the project.

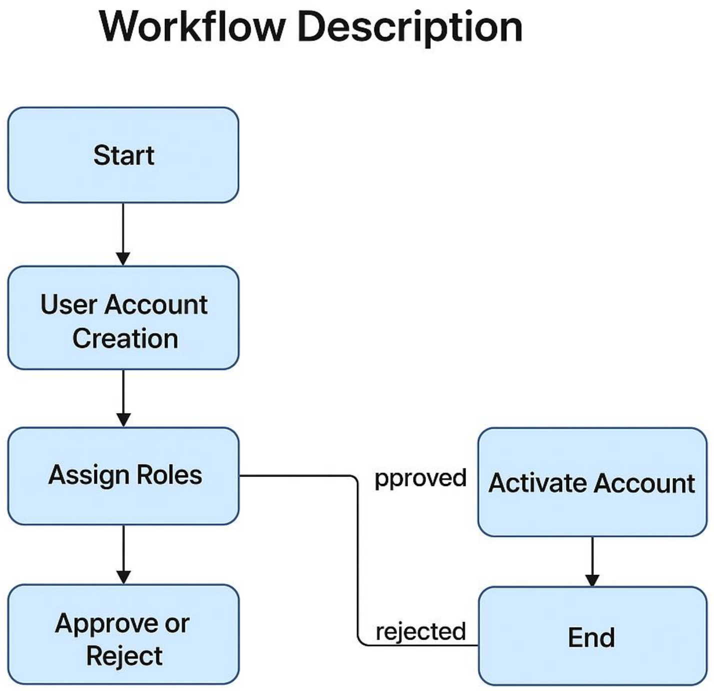
After the roles are defined, the request progresses to the **Approval or Rejection** stage. Here, the system sends the request to the administrator or project manager for verification. The approver can review the details, validate the user's role, and either approve or reject the request. If the request is approved, the system automatically proceeds to **Activate Account**, granting the user necessary permissions and access to the assigned modules or tasks. In case of rejection, the workflow ends with a notification to the user, indicating the reason for denial.

The automated workflow eliminates the need for manual tracking and communication. It ensures that all approvals are documented and that role assignments are handled securely and efficiently. Furthermore, the system can generate reports and logs for auditing purposes, allowing administrators to monitor user activity and project access history.

Overall, this workflow provides an efficient, transparent, and secure process for managing user and project-related operations within the ServiceNow environment. It reduces human dependency, enhances accountability, and aligns with organizational IT Service Management (ITSM) best practices.

11. DATA FLOW DIAGRAM:

The Data Flow Diagram (DFD) illustrates how user requests move through the system. Input data (requests) is validated, approved, and stored in the database. Data then flows to dashboards for visualization.



12. IMPLEMENTATION

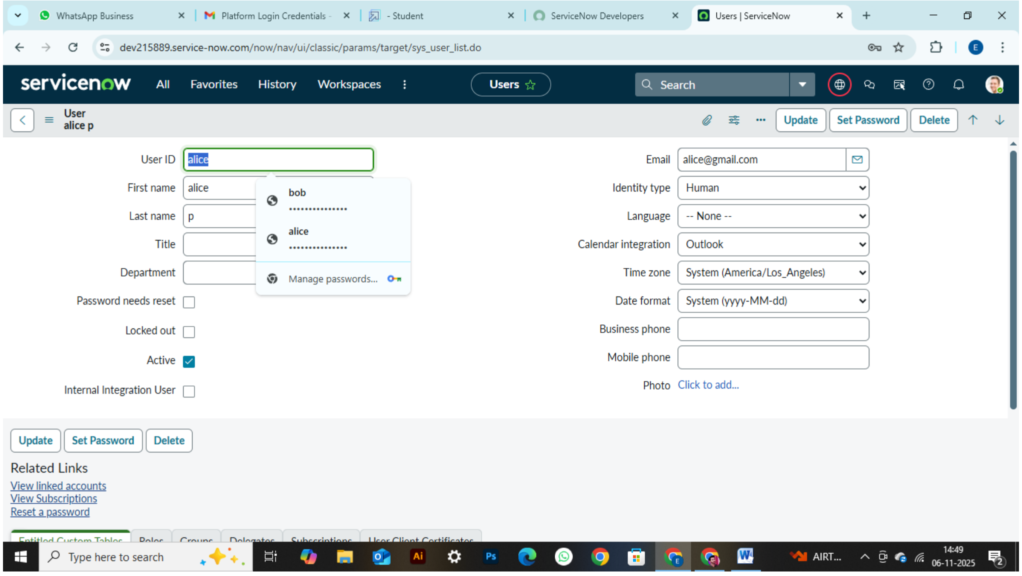
The implementation is done using ServiceNow modules:

1. Users

The first step in the implementation is the creation of user accounts within the ServiceNow platform. Each user profile contains critical information such as the user's name, email address, department, and user ID. This data helps in uniquely identifying each person in the system. Users can represent employees, team members, or administrators who require access to perform their duties.

Creating users is done through the User Table (sys_user) in ServiceNow. Administrators can either manually create users or import them from an existing employee database. Each user entry is verified before being activated in the system. Properly managing user records ensures accountability and a clear structure for assigning access rights and responsibilities.

1. Create the alice user:

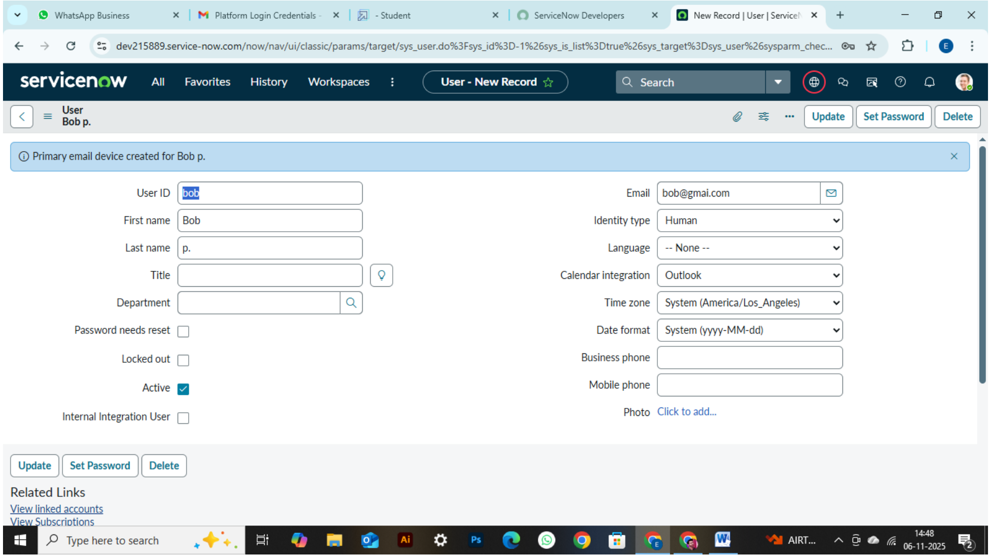


dev215889.service-now.com/now/nav/ui/classic/params/target/sys_user_list.do

User
alice p

User ID	alice
First name	alice
Last name	p
Title	
Department	
Password needs reset	□
Locked out	□
Active	☑
Internal Integration User	□
Email	alice@gmail.com
Identity type	Human
Language	-- None --
Calendar integration	Outlook
Time zone	System (America/Los_Angeles)
Date format	System (yyyy-MM-dd)
Business phone	
Mobile phone	
Photo	Click to add...

2. Create the bob user :



dev215889.service-now.com/now/nav/ui/classic/params/target/sys_user.do%3Fsys_id%3D-1%26sys_is_list%3Dtrue%26sys_target%3Dsys_user%26sysparm_chec...

User
Bob p.

Primary email device created for Bob p.

User ID: bob
First name: Bob
Last name: p.
Title:
Department:
Password needs reset: □
Locked out: □
Active: ☑
Internal Integration User: □

Email: bob@gmai.com
Identity type: Human
Language: -- None --
Calendar integration: Outlook
Time zone: System (America/Los_Angeles)
Date format: System (yyyy-MM-dd)
Business phone:
Mobile phone:
Photo: Click to add...

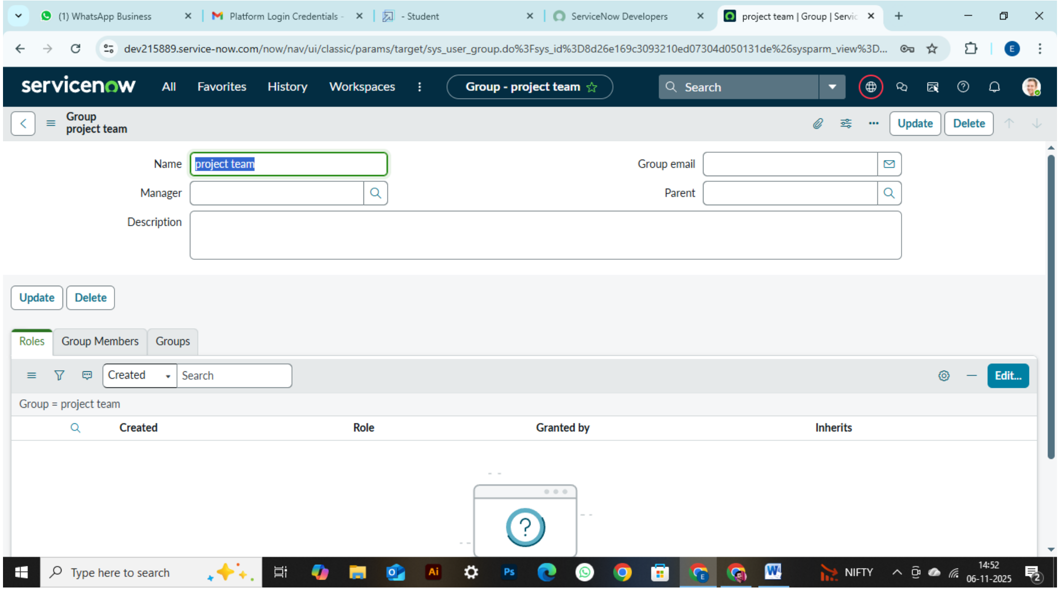
Related Links
View linked accounts
View Subscriptions

2.Groups:

Groups are essential for managing multiple users with similar job roles or project responsibilities. A **group** acts as a logical collection of users who can share access permissions, tasks, or projects. For example, all team members working on a particular project can be added to one group called "Project A Team."

In ServiceNow, groups are stored in the **sys_user_group** table. When a group is created, it becomes easier to assign roles or tickets collectively instead of assigning them individually. Groups also play a crucial role in workflows where an entire department, such as "IT Support," needs to receive and resolve incident tickets.

1. Create the Groups:



dev215889.service-now.com/now/nav/ui/classic/params/target/sys_user_group.do%3Fsys_id%3D8d26e169c3093210ed07304d050131de%26sysparm_view%3D...

Group
project team

Name: project team
Manager:
Description:
Group email:
Parent:

Group = project team

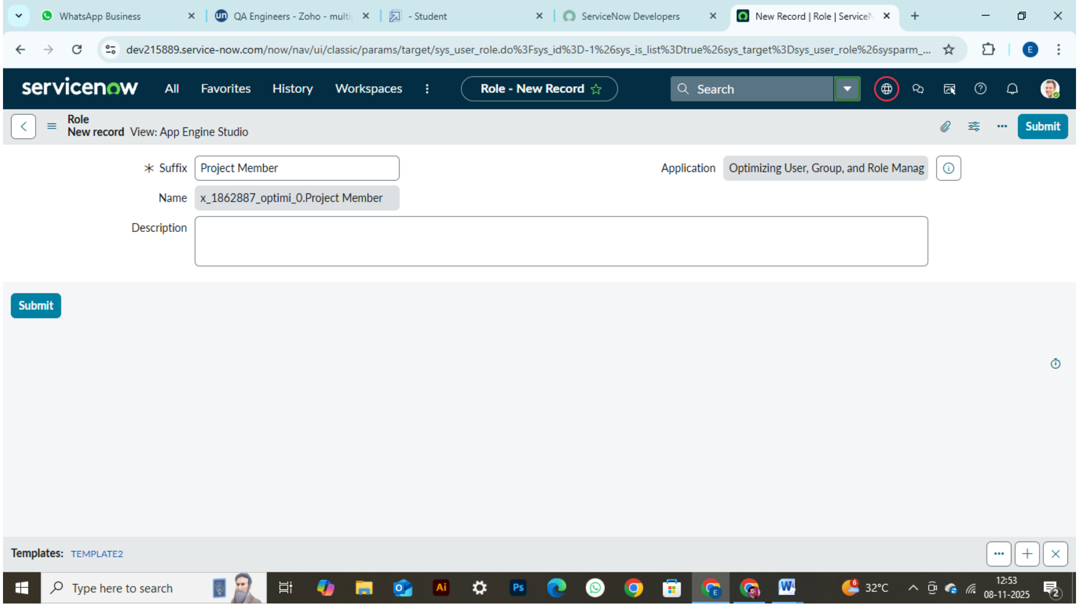
Created	Role	Granted by	Inherits

3.Roles:

Roles define the **level of access and privileges** that a user or group has within the system. Each role is associated with specific permissions that control what actions a user can perform. Examples include roles like *admin*, *itil (IT Service Management)*, *hr_admin*, and *project_manager*.

By assigning the correct roles, administrators ensure that sensitive data and operations are protected. For instance, an admin can create and modify records, whereas a project member may only view or update assigned tasks. Roles are stored in the **sys_user_role** table, and multiple roles can be linked to one user depending on their function.

1. Create the Roles:



dev215889.service-now.com/now/nav/ui/classic/params/target/sys_user_role.do%3Fsys_id%3D-1%26sys_is_list%3Dtrue%26sys_target%3Dsys_user_role%26sysparm_...

Role - New Record

Role
New record View: App Engine Studio

* Suffix	Project Member
Name	x_1862887_optimi_0.Project Member
Description	
Application	Optimizing User, Group, and Role Manag

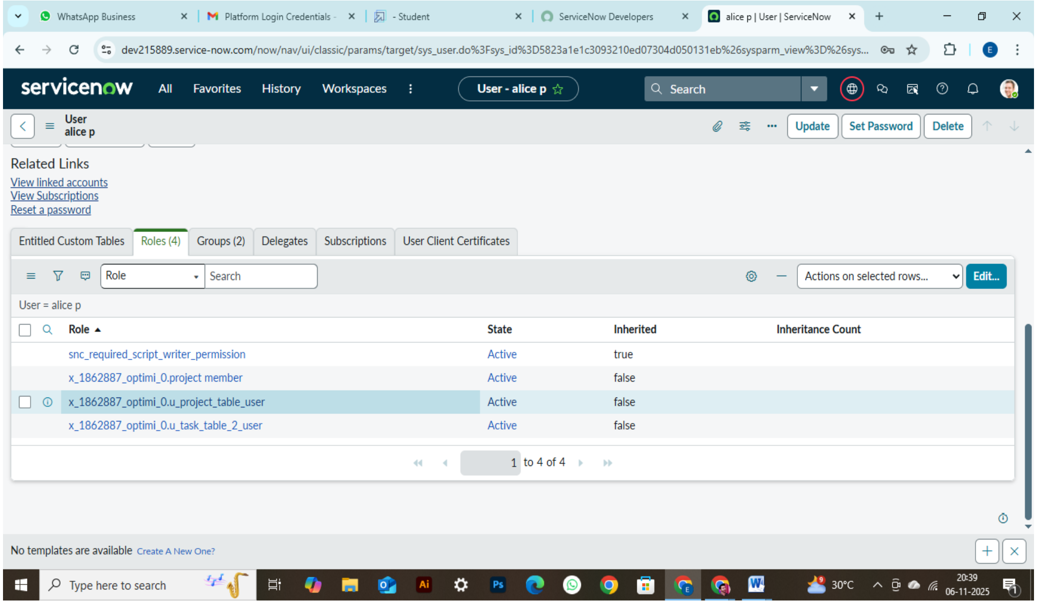
Templates: TEMPLATE2

4.Assign Users to Groups:

Once users and groups are created, the next step is to **assign users to their respective groups**. This helps organize members efficiently according to projects or departments. For example, *Alice* and *Bob* can be added to the *Development Team* group.

This assignment simplifies task management and approval processes. When an incident or project task is created, it can be automatically assigned to a specific group rather than an individual. The system uses this mapping to route workflows efficiently, improving team collaboration and reducing response times.

1. Assign Roles to Alice User :



User
alice p

Related Links
View linked accounts
View Subscriptions
Reset a password

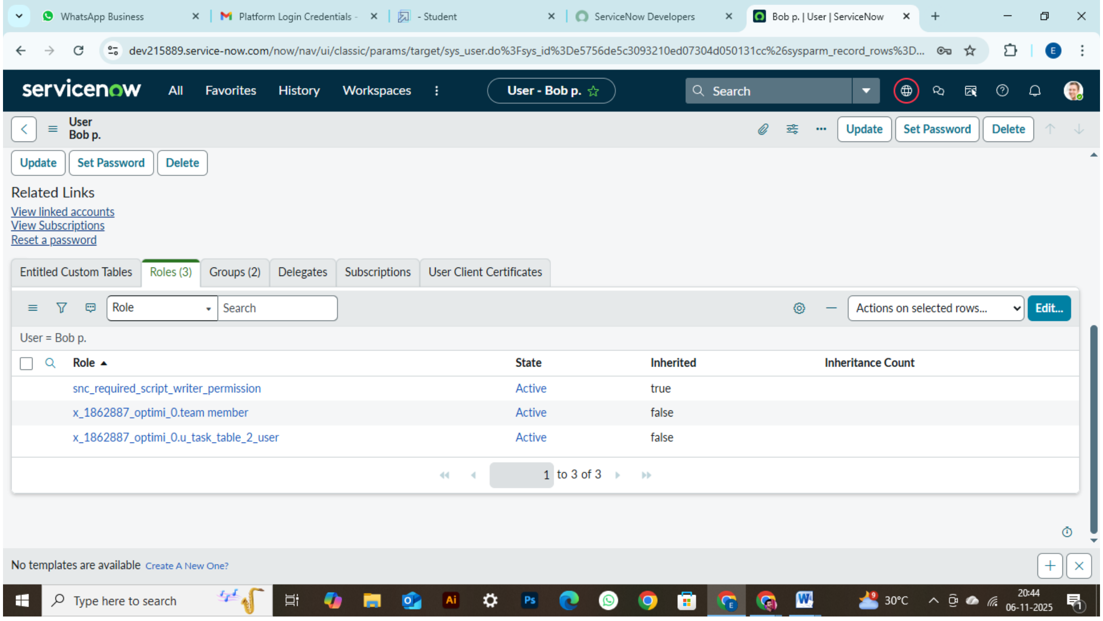
User = alice p

Role ▲	State	Inherited	Inheritance Count
snc_required_script_writer_permission	Active	true	
x_1862887_optimi_0.project member	Active	false	
x_1862887_optimi_0.u_project_table_user	Active	false	
x_1862887_optimi_0.u_task_table_2_user	Active	false	

1 to 4 of 4

No templates are available Create A New One?

2.Assign Roles to Bob User :



User
Bob p.

Related Links
View linked accounts
View Subscriptions
Reset a password

User = Bob p.

Role ▲	State	Inherited	Inheritance Count
snc_required_script_writer_permission	Active	true	
x_1862887_optimi_0.team member	Active	false	
x_1862887_optimi_0.u_task_table_2_user	Active	false	

1 to 3 of 3

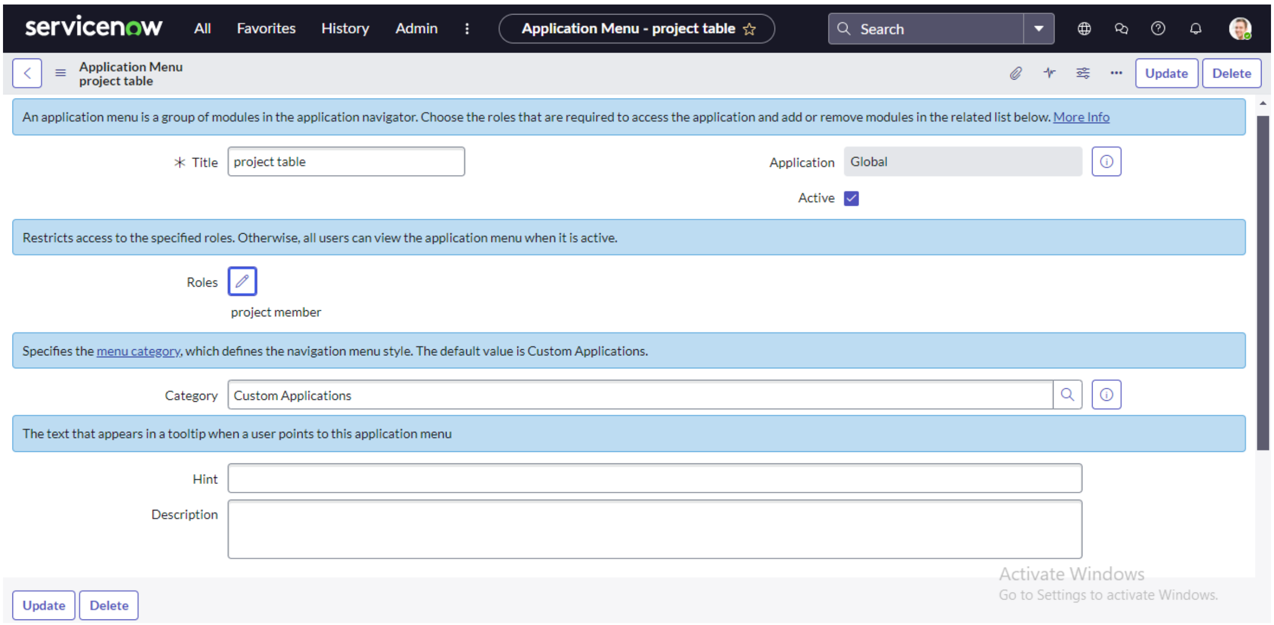
No templates are available Create A New One?

5.Application Access

The **Application Access** module defines which users, roles, or groups can access specific applications within the ServiceNow environment. By default, not every user can access all applications. Administrators configure access restrictions at the application level to safeguard sensitive modules.

This step helps prevent misuse and unauthorized entry into modules like HR, Finance, or IT Service Management. Assigning appropriate application access enhances security and ensures that users only interact with data relevant to their duties.

1.Assign table access to application:



Application Menu
project table

An application menu is a group of modules in the application navigator. Choose the roles that are required to access the application and add or remove modules in the related list below. More Info

✱ Title	project table	Application	Global
		Active	☑

Restricts access to the specified roles. Otherwise, all users can view the application menu when it is active.

Roles: project member

Specifies the menu category, which defines the navigation menu style. The default value is Custom Applications.

Category: Custom Applications

The text that appears in a tooltip when a user points to this application menu

Hint:

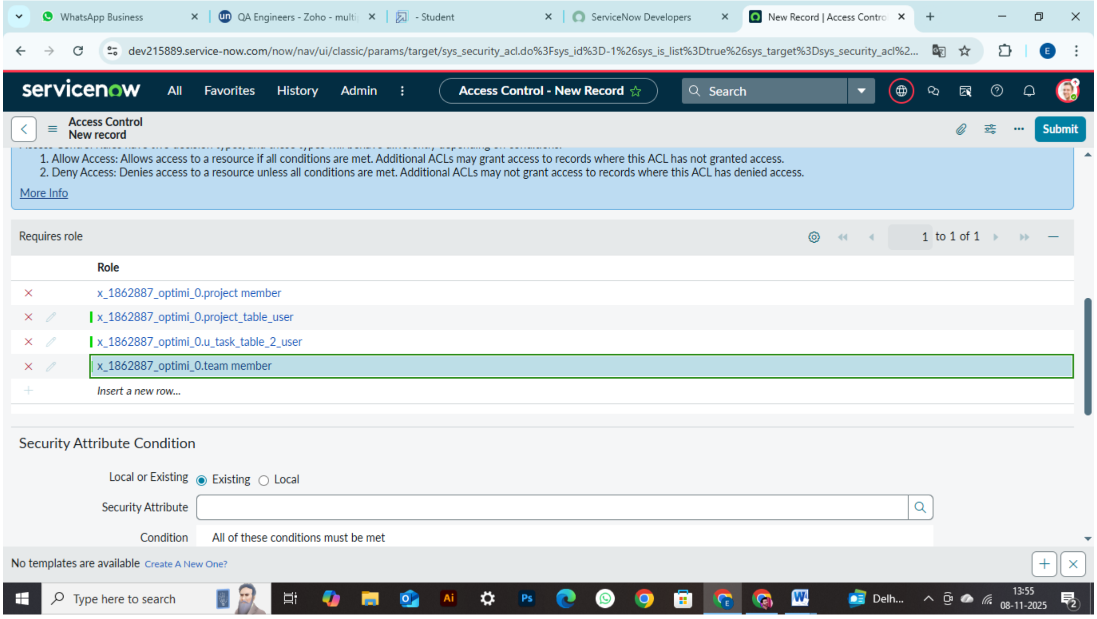
Description:

6. Assign Table Access to Application :

In this step, administrators configure **table-level access controls** to ensure proper data protection. ServiceNow applications often contain multiple tables (like `incident`, `task`, or `request`), and each table may have sensitive information.

By assigning access to specific tables, administrators ensure that users can only read, write, or update records that pertain to their work. For instance, a project member can view their own tickets but not modify another team's data. This fine-grained access management aligns with data confidentiality standards.

1.**Create ACL:**



WhatsApp Business
QA Engineers - Zoho - multi
- Student
ServiceNow Developers
New Record | Access Contro
dev215889.service-now.com/now/nav/ui/classic/params/target/sys_security_acl.do%3Fsys_id%3D-1%26sys_is_list%3Dtrue%26sys_target%3Dsys_security_acl%2...
servicenow
All
Favorites
History
Admin
Access Control - New Record
Search
Submit

Access Control
New record

1. Allow Access: Allows access to a resource if all conditions are met. Additional ACLs may grant access to records where this ACL has not granted access.
2. Deny Access: Denies access to a resource unless all conditions are met. Additional ACLs may not grant access to records where this ACL has denied access.

More Info

Requires role — 1 to 1 of 1

Role
x_1862887_optimi_0.project member
x_1862887_optimi_0.project_table_user
x_1862887_optimi_0.u_task_table_2_user
x_1862887_optimi_0.team member
Insert a new row...

Security Attribute Condition

Local or Existing ● Existing ○ Local

Security Attribute

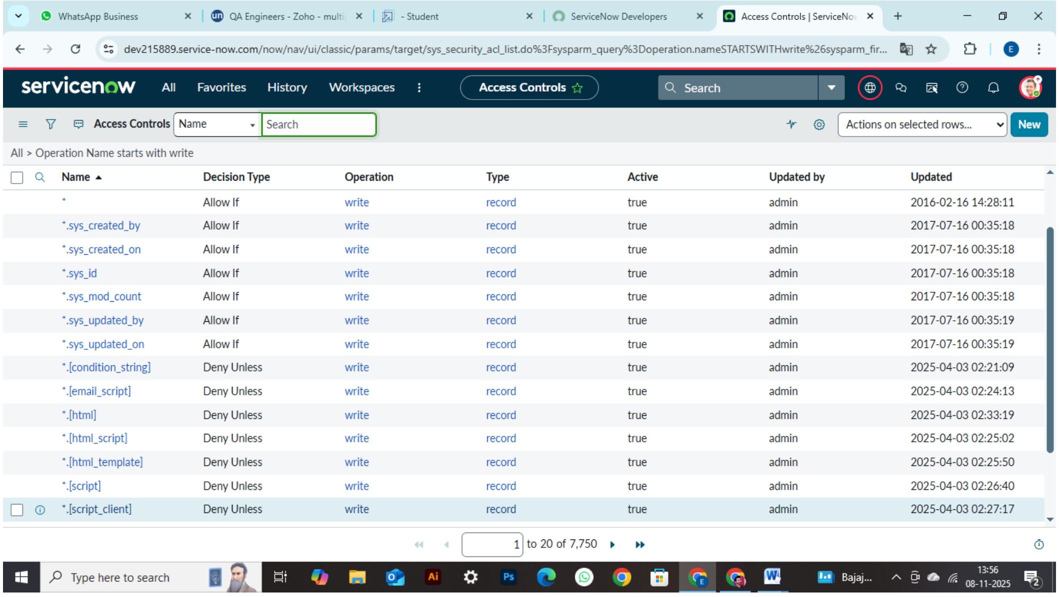
Condition All of these conditions must be met

No templates are available Create A New One?

7. Access Control List (ACL)

Access Control Lists (ACLs) are one of the most powerful features in ServiceNow. They provide detailed control over what data a user can view or modify at the **record or field level**. ACLs evaluate user roles, conditions, and scripts before granting access to a record.

For example, an ACL rule can be set so that only users with the *manager* role can approve requests, while others can only view them. Implementing ACLs ensures system-wide data protection and adherence to organizational policies.


dev215889.service-now.com/now/nav/ui/classic/params/target/sys_security_acl_list.do%3Fsysparm_query%3Doperation.nameSTARTSWITHwrite%26sysparm_fir...
servicenow
All
Favorites
History
Workspaces
Access Controls
Search
Access Controls
Name
Search
Actions on selected rows...
New

All > Operation Name starts with write

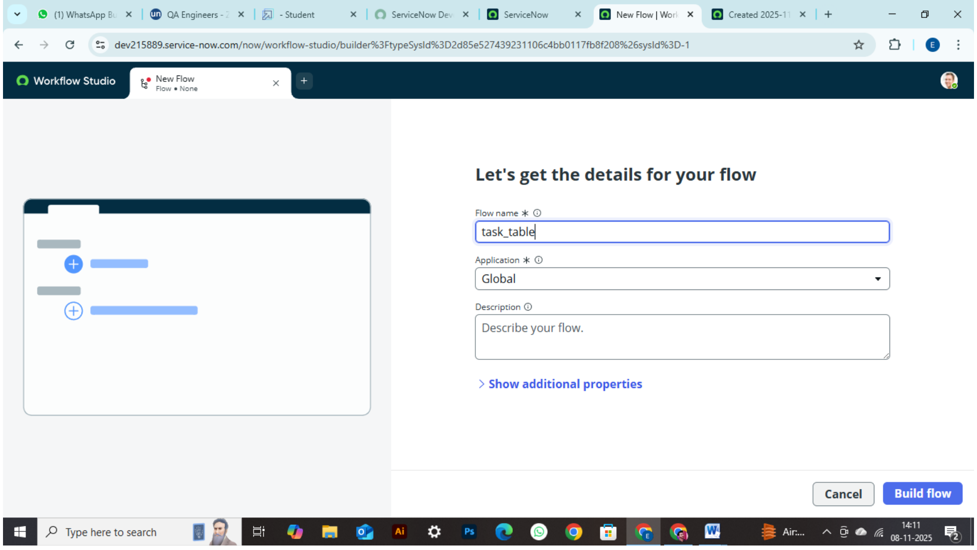
Name ▲	Decision Type	Operation	Type	Active	Updated by	Updated
*	Allow If	write	record	true	admin	2016-02-16 14:28:11
*.sys_created_by	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_created_on	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_id	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_mod_count	Allow If	write	record	true	admin	2017-07-16 00:35:18
*.sys_updated_by	Allow If	write	record	true	admin	2017-07-16 00:35:19
*.sys_updated_on	Allow If	write	record	true	admin	2017-07-16 00:35:19
*.[condition_string]	Deny Unless	write	record	true	admin	2025-04-03 02:21:09
*.[email_script]	Deny Unless	write	record	true	admin	2025-04-03 02:24:13
*.[html]	Deny Unless	write	record	true	admin	2025-04-03 02:33:19
*.[html_script]	Deny Unless	write	record	true	admin	2025-04-03 02:25:02
*.[html_template]	Deny Unless	write	record	true	admin	2025-04-03 02:25:50
*.[script]	Deny Unless	write	record	true	admin	2025-04-03 02:26:40
*.[script_client]	Deny Unless	write	record	true	admin	2025-04-03 02:27:17

1 to 20 of 7,750

8.Flows:

ServiceNow’s **Flow Designer** is used to automate business processes without the need for coding. A flow is a series of actions that are triggered based on certain conditions. This automation reduces manual workload and increases consistency in handling repetitive tasks.

For example, when a new user joins the organization, a flow can automatically create their account, assign roles, and notify the admin. The drag-and-drop interface in Flow Designer makes it easy to design, test, and manage workflows seamlessly.


dev215889.service-now.com/now/workflow-studio/builder%3FtypeSysId%3D2d85e527439231106c4bb0117fb8f208%26sysId%3D-1
Workflow Studio
New Flow
Flow • None
Cancel
Build flow

Let's get the details for your flow

Flow name *: task_table

Application *: Global

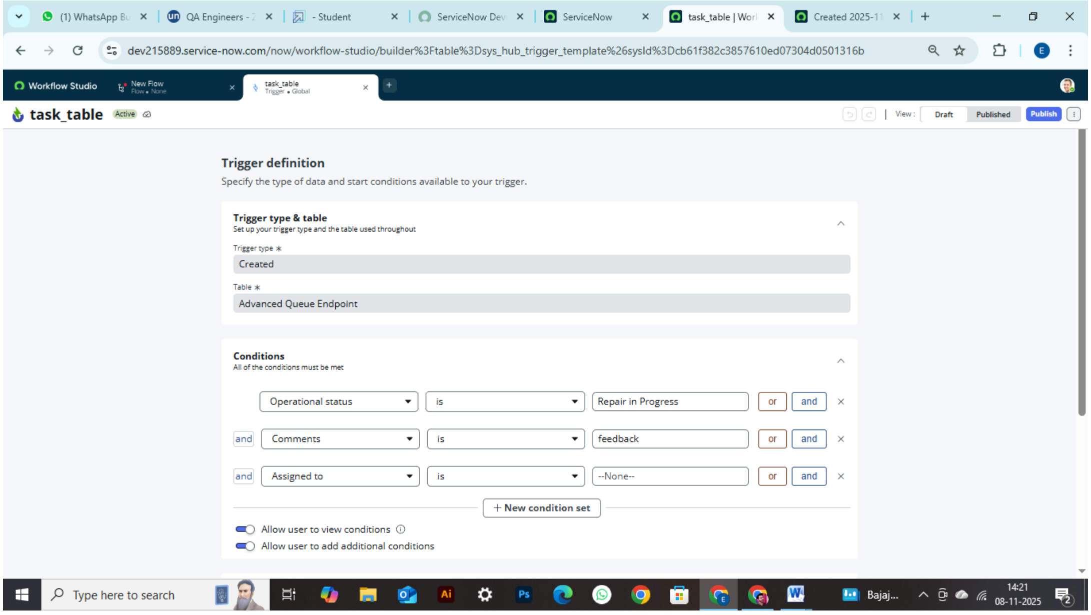
Description: Describe your flow.

> Show additional properties

9. Create a Flow to Assign Operations Ticket to Group:

In this implementation, a specific flow is created to **automatically assign Operations tickets to a group**. When a new ticket is generated (for example, a server issue or software bug), the system triggers the flow, which checks predefined conditions and routes the ticket to the appropriate group, such as "IT Operations."

This automation ensures that no ticket is left unattended and that the correct team handles the issue immediately. It enhances productivity, reduces delays, and ensures smooth coordination across teams.



dev215889.service-now.com/now/workflow-studio/builder%3Ftable%3Dsys_hub_trigger_template%26sysId%3Dcb61f382c3857610ed07304d0501316b

task_table Active

Trigger definition

Specify the type of data and start conditions available to your trigger.

Trigger type & table

Set up your trigger type and the table used throughout

Trigger type *: Created

Table *: Advanced Queue Endpoint

Conditions

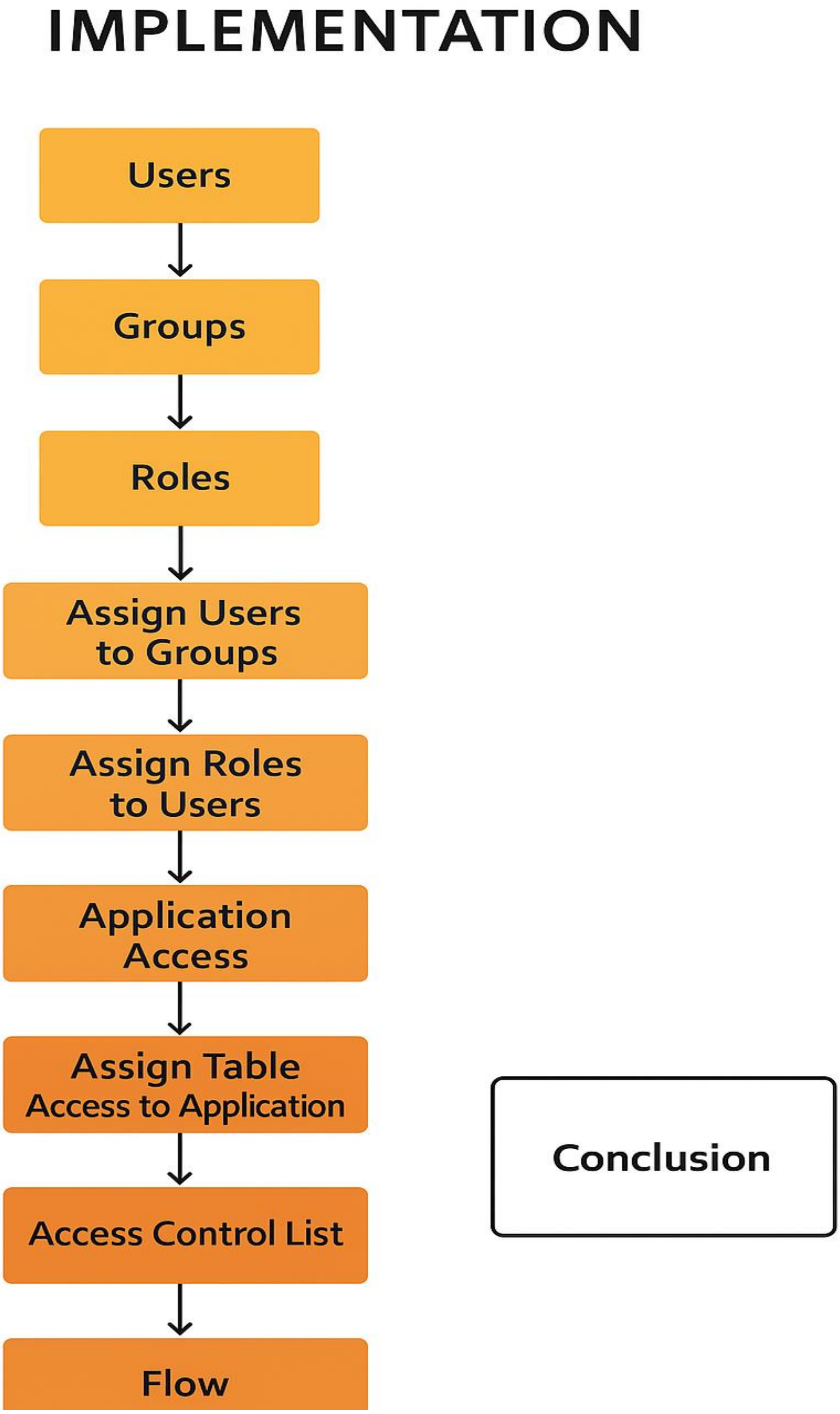
All of the conditions must be met

	Operational status	is	Repair in Progress
and	Comments	is	feedback
and	Assigned to	is	--None--

Allow user to view conditions

Allow user to add additional conditions

FLOW DIAGRAM:



13.ACCESS CONTROL CONFIGURATION :

Access control configuration is one of the most crucial components in the **ServiceNow platform** to ensure that only authorized users can view, modify, or delete information within the system. It safeguards sensitive data, enforces role-based security, and helps organizations maintain compliance with their internal and external security policies.

In this project, **Access Control Lists (ACLs)** are implemented to define precise permissions at different levels—table, record, and field. Each ACL rule determines whether a user can perform actions such as *read*, *write*, *create*, or *delete* on specific data. These rules are based on three primary factors: **roles**, **conditions**, and **scripts**. For example, a rule can be configured so that only users with the *admin* or *project_manager* role can update records in the "Project Task" table, while regular users can only view them.

The configuration begins with identifying all the essential tables that require restricted access, such as **User**, **Group**, and **Task**. For each of these tables, access permissions are defined according to organizational needs. Administrators use the **Access Control (sys_security_acl)** module to create or modify these rules. ServiceNow evaluates ACLs in a top-down order, ensuring that the most specific rule is applied first.

To strengthen security, **Application Access Settings** are also configured. These settings define which roles can access specific application modules or tables, preventing unauthorized users from entering restricted areas of the system. Additionally, access to related lists and forms is restricted to prevent accidental or unauthorized data exposure.

Once all ACLs and application access rules are configured, thorough testing is conducted. Different user profiles—such as administrators, managers, and team members—are used to validate that the access control settings are functioning as expected. This ensures that each user type has the correct permissions aligned with their responsibilities.

Overall, the **Access Control Configuration** provides a secure, structured, and role-based access environment. It minimizes security risks, prevents data misuse, and ensures that users interact only with the information they are authorized to handle. This configuration reinforces accountability, supports workflow automation, and enhances the integrity of the ServiceNow system.

14. USER ROLES AND PERMISSIONS MATRIX

In ServiceNow**,** user roles and permissions define the level of access and control each user has within the system. The User Roles and Permissions Matrix serves as a blueprint that outlines which roles can perform specific actions on tables, applications, and modules. This structure ensures accountability, maintains data security, and prevents unauthorized operations.

The configuration starts by identifying the different categories of users involved in the project. In this implementation, the primary roles are Administrator**,** Project Manager**,** Team Member**,** and End User. Each role carries distinct privileges designed to match the user's responsibilities within the system.

1. **Administrator** – This role has full system privileges, including creating and modifying tables, designing workflows, managing ACLs, and assigning roles. Administrators are responsible for maintaining the overall platform, troubleshooting errors, and ensuring smooth operation of the ServiceNow environment.
2. **Project Manager** – Project Managers have access to create, update, and assign tasks related to projects. They can view all project records, monitor progress, and approve or reject requests. However, they cannot modify system settings or access administrative modules.
3. **Team Member** – Team Members can view and update only the tasks assigned to them. They can add comments, upload attachments, and mark tasks as complete. Their permissions are limited to operational-level activities, ensuring they cannot alter project configurations or affect other users' data.
4. **End User** – This is the most restricted role, typically assigned to employees or clients who submit requests or incidents. End Users can create new requests, view their own submissions, and track status updates. They do not have access to administrative or project management features.

The Permissions Matrix is implemented using Access Control Rules (ACLs) and Role Assignments**.** Each module and table is mapped against the corresponding roles to specify actions such as *read*, *write*, *create*, and *delete*. Regular audits and testing are conducted to verify that these permissions align with security standards and organizational policies.

15. TESTING

Testing is a crucial phase in the development and deployment of the project **“Optimizing User, Group, and Role Management with Access Control and Workflows”**. The main objective of testing is to ensure that all functionalities—such as user creation, role assignment, access control, and automated workflows—operate correctly and efficiently within the **ServiceNow platform**. This phase also verifies that the system meets the defined requirements, performs reliably, and provides a secure user experience.

Testing began after the configuration and implementation stages were completed. Various testing methods were employed to validate each component of the system:

1. Unit Testing

Each module—such as User Management**,** Group Creation**,** Role Assignment, and Access Control Configuration**—**was tested independently to verify that it performs its intended function without errors. Unit testing ensured that database interactions, form designs, and ACL configurations worked as expected before integrating the modules together.

2. Integration Testing

After unit testing, all modules were integrated and tested as a whole system. Integration testing ensured that the flow between different modules (for example, assigning roles to users or creating tasks automatically through workflows) was seamless. This phase confirmed that data passed correctly between tables and workflows triggered under proper conditions.

3. Functional Testing

Functional testing focused on verifying that the system met all project requirements. Test cases were created for operations like adding new users, assigning roles, restricting unauthorized access, and validating approval flows. This testing confirmed that all buttons, forms, and notifications behaved as designed.

4. Security and Access Control Testing

This testing ensured that **the** Access Control Lists (ACLs) and Application Access Settings were properly enforced. Multiple test users with different roles (Admin, Manager, and Team Member) were used to verify that each had only the permissions assigned to them. Unauthorized attempts to access restricted modules were blocked, confirming that security policies were correctly applied.

5. User Acceptance Testing (UAT)

Finally, end-users and administrators reviewed the system to confirm usability, reliability, and performance. Feedback from this phase helped refine minor configurations and optimize workflows for better user experience.

16. RESULTS AND DISCUSSION

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” was successfully implemented and tested on the **ServiceNow platform**. The results demonstrate that the designed system effectively automates user administration, enforces access control, and enhances workflow efficiency across the organization.

1. Improved User and Role Management

After implementation, administrators could create, update, and deactivate users more efficiently using a single centralized interface. The automated mapping between users, groups, and roles significantly reduced manual intervention. Tasks that earlier required multiple steps—such as assigning permissions or managing access requests—were now handled automatically through predefined workflows. This improvement led to fewer human errors and consistent application of security policies.

2. Enhanced Security through Access Control Lists (ACLs)

The Access Control Configuration successfully restricted unauthorized access to data and applications. Each user was granted privileges strictly according to their assigned role. During testing, users with limited roles could not view or modify restricted data, confirming that ACLs and role-based permissions were functioning as expected. This reinforced data integrity, confidentiality, and accountability within the system.

3. Workflow Automation and Task Management

The use of **Flow Designer** automated repetitive processes, such as approvals and ticket assignments. For example, when a new operations ticket was created, it was automatically assigned to the relevant group without any manual input. This automation reduced task resolution time, improved transparency, and ensured that no request was overlooked.

4. System Performance and User Experience

Performance evaluation indicated that the system responded quickly and handled concurrent operations without delays. Administrators and project managers reported that the dashboard interface was intuitive and easy to navigate. The structured design of workflows and clear visibility into user roles provided a more controlled and transparent environment.

5. Discussion

The outcomes confirm that ServiceNow is an effective platform for implementing automated access control and workflow management. The integration of ACLs, Flow Designer, and user management modules delivers a scalable and secure IT service management solution. Moreover, the system’s modular design allows future expansion, such as integrating incident management or HR service modules.

17. ADVANTAGES

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” developed on the ServiceNow platform offers several advantages that improve system efficiency, security, and automation within an organization.

1. Automation of Manual Processes

One of the most significant benefits is the automation of repetitive administrative tasks. Activities such as creating users, assigning roles, and managing approvals are streamlined through **Flow Designer** workflows. This automation minimizes human intervention, reduces the risk of errors, and saves valuable administrative time.

2. Enhanced Security

By implementing **Access Control Lists (ACLs)** and role-based permissions, the system ensures that users have access only to authorized data and modules. This strict access control mechanism prevents data breaches, safeguards sensitive information, and enforces compliance with organizational security policies.

3. Centralized User Management

ServiceNow provides a unified platform for managing users, roles, and groups. Administrators can easily track user activities, update permissions, and monitor access logs, thereby improving accountability and transparency.

4. Improved Workflow Efficiency

Automated task assignments and approval processes enhance productivity. Tickets are automatically routed to the right groups or individuals, ensuring faster response times and better service delivery.

5. Scalability and Flexibility

The system’s modular design allows easy expansion to support additional business processes, such as incident or project management, without major reconfiguration.

Overall, the project demonstrates how automation and access control within ServiceNow can transform traditional administrative systems into efficient, secure, and scalable digital workflows.

18. APPLICATIONS

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” developed on the ServiceNow platform has a wide range of applications across industries and organizations that rely on secure and efficient IT service management systems.

1. IT Service Management (ITSM)

This project can be directly applied in IT service environments to manage employee accounts, assign tickets, and control access to IT resources. Automated workflows can handle incident creation, task assignment, and approval processes, thereby improving operational efficiency and reducing response times.

2. Human Resource Management

The system can be extended to automate HR functions such as onboarding and offboarding employees. When a new employee joins, the workflow can automatically create their user account, assign appropriate roles, and grant access to necessary modules. Similarly, access can be revoked automatically during offboarding, ensuring data security.

3. Project and Team Management

Organizations can use this system to organize users into project-based groups, assign responsibilities, and track progress through workflow automation. Project managers can monitor tasks, review approvals, and ensure accountability for each member.

4. Educational and Training Institutions

Institutions can apply this system to manage staff, students, and administrative access to digital resources. Role-based controls ensure that teachers, students, and administrators have access to their respective modules only.

5. Enterprise Security Management

Companies can implement this solution to maintain strict role-based data security, preventing unauthorized access and ensuring compliance with data protection policies.

19. FUTURE ENHANCEMENTS:

While the project “Optimizing User, Group, and Role Management with Access Control and Workflows” successfully achieves automation, security, and efficiency in user management, there remains significant potential for future improvements. These enhancements can further expand the system’s capabilities and adaptability to evolving business needs and technological advancements.

1. Integration with Other Modules

Future versions of the system can be integrated with other ServiceNow applications such as *Incident Management*, *Change Management*, and *Problem Management*. This would allow seamless data flow between modules, enabling a more holistic IT service management experience and reducing manual coordination between teams.

2. Advanced Analytics and Reporting

Introducing advanced analytics can help administrators generate detailed reports on user activity, access patterns, and workflow performance. Dashboards with real-time insights would support better decision-making and proactive management of user privileges and system usage.

3. Artificial Intelligence (AI) and Predictive Automation

AI can be incorporated to predict workflow bottlenecks and automatically recommend process optimizations. Machine learning algorithms could analyze access data to identify unusual behavior or potential security threats, improving overall system intelligence and security.

4. Mobile Accessibility

Developing a mobile-friendly interface or a dedicated ServiceNow mobile app extension would allow administrators and users to access workflows, approvals, and tickets anytime, anywhere. This enhancement would significantly improve flexibility and productivity for remote teams.

5. Self-Service Portal Enhancements

Adding more self-service functionalities can empower end users to request role changes, reset passwords, or generate reports independently, further reducing administrative workload and improving user satisfaction.

6. Integration with External Systems

Future updates could connect the system with external HR, ERP, or CRM tools to synchronize user data automatically, ensuring consistency across all organizational platforms.

20.CONCLUSION:

The project “Optimizing User, Group, and Role Management with Access Control and Workflows” successfully demonstrates how the ServiceNow platform can be utilized to automate administrative processes, enhance security, and improve efficiency within an organization. The system was designed to address common challenges in manual user management, such as data inconsistency, human error, and security risks caused by uncontrolled access.

Through the implementation of Access Control Lists (ACLs), role-based permissions, and Flow Designer workflows, the project achieved a fully automated and structured user management process. Administrators can now manage users, roles, and groups more efficiently, while ensuring that every user interacts only with data and modules relevant to their role. This structure promotes accountability, transparency, and strong compliance with organizational policies.

Testing and evaluation confirmed that the system performs reliably under different conditions. Workflows such as automatic task assignment and approval routing significantly reduced manual effort and turnaround time. The role-based access control model ensured that sensitive information remained protected, fulfilling one of the project’s core objectives — secure and efficient access management.

Moreover, the modular design of the project makes it scalable for future integration with other ServiceNow applications such as Incident Management, HR Services, and Asset Management. The success of this implementation highlights the potential of ServiceNow as a robust platform for digital transformation and process automation.

In conclusion, the project has effectively optimized user, group, and role management through secure access controls and intelligent workflows, contributing to a more efficient, reliable, and secure IT service management environment.

21. BIBLIOGRAPHY

- ServiceNow Documentation – *ServiceNow Product Documentation Portal*, https://docs.servicenow.com

- ServiceNow Developer Site – *ServiceNow Developer Program*, https://developer.servicenow.com

- ServiceNow Community – *Discussions, Blogs, and Technical Articles*, https://community.servicenow.com

- ServiceNow Learning Portal – *ServiceNow Training and Certification Resources*, https://nowlearning.servicenow.com

- Turbeville, M. (2021). *Learning ServiceNow: Administration and Development Made Simple*. Packt Publishing.

- Bhatia, S. (2020). *Mastering ServiceNow Scripting*. Packt Publishing.

- ITIL Foundation. (2019). *ITIL 4 Foundation: IT Service Management Framework.* AXELOS.

- Sharma, A., & Gupta, R. (2021). *Implementing IT Service Management with ServiceNow*. Apress.

- Udemy Course – *ServiceNow Administration and Development Bootcamp*, https://www.udemy.com

- ServiceNow Wiki Archives – *Access Control Rules, Roles, and Workflows Overview*.