

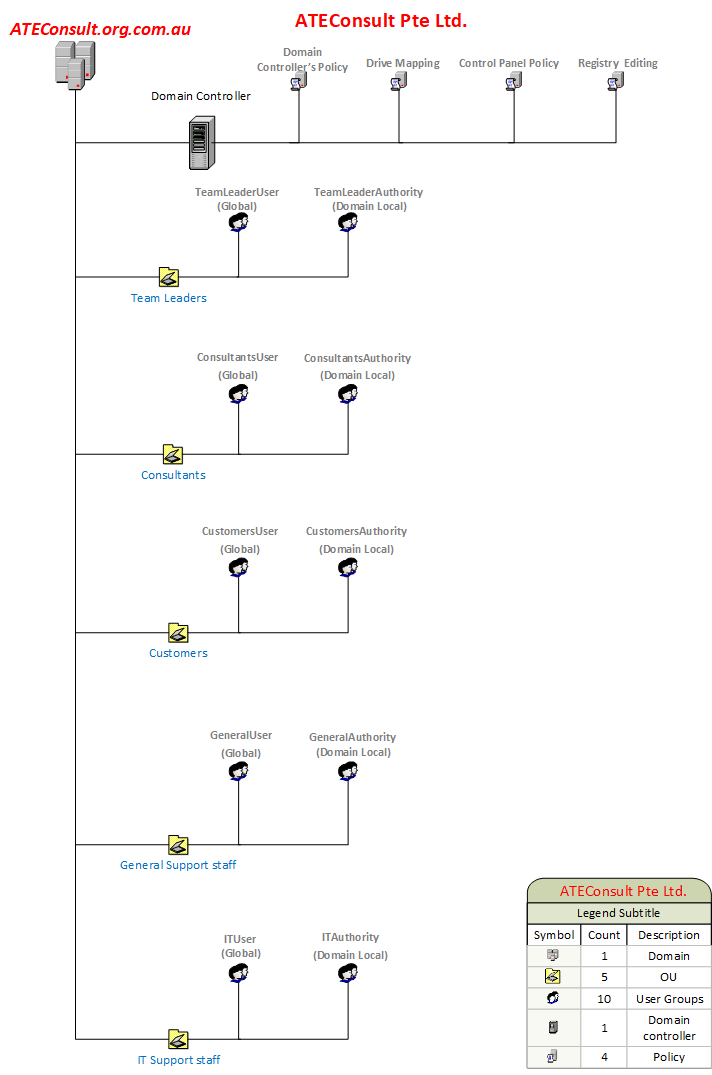
INFT2031

Network & System Administration

Assignment 2

ATEConsult Pte Ltd – Active design

The first thing I’ve done here that I create a domain to manage all resources for ATEConsult Pte Ltd and set the Domain name as *“ATEConsult.org.com.au”*



**ATEConsult Pte Ltd is a small consultancy firm located in Charlestown. ATEConsult’s IT resources span a number of Windows 10 machines and a Windows Server 2016 server. You are hired as the IT consultant to design the Active Directory logical structure for ATEConsult.**

**Requirement 1:**

***There are five major categories of users: Team Leaders, Consultants, Customers, General***

***Support staff and IT Support staff.***

I create OU’s for each category of users under the domain and use the AGDLP guidelines to create user groups for ATEConsult Pte Ltd ’s domain users.

* Team Leader
* Consultants
* Customers
* General Support Staff
* IT Support Staff

I create two user groups for each OU and give permissions mention as “Authority” in the design.

**Requirement 2:**

***Create appropriate user groups to provide access to resources of different users’ groups.***

I am explaining that by drawing a table below:

|  |  |  |  |
| --- | --- | --- | --- |
| Group | Group Type | Members | Short Description |
| TeamLeaderUser | Global | User accounts of Team Leaders | This group contains all Team Leaders user accounts |
| TeamLeaderAuthority | Domain Local | TeamLeaderUsers | This group contains all permissions and privileges for Team Leaders in ATEConsult Pte Ltd domain |
| ConsultantsUser | Global | User accounts of Consultants | This group contains all Consultants user accounts |
| ConsultantsAuthority | Domain Local | ConsultantsUsers | This group contains all permissions and privileges for Consultants in ATEConsult Pte Ltd domain |
| CustomersUser | Global | User accounts of Customers | This group contains all Customers user accounts |
| CustomersAuthority | Domain Local | CustomersUsers | This group contains all permissions and privileges for Customers in ATEConsult Pte Ltd domain |
| GeneralUser | Global | User accounts of GeneralSupportStaff | This group contains all GeneralSupportStaff user accounts |
| GeneralAuthority | Domain Local | GeneralSupportStaffUsers | This group contains all permissions and privileges for GeneralSupportStaff in ATEConsult Pte Ltd domain |
| ITUser | Global | User accounts of ITSupportStaff | This group contains all ITSupportStaff user accounts |
| ITAuthority | Domain Local | ITSupportStaffUsers | This group contains all permissions and privileges for ITSupportStaff in ATEConsult Pte Ltd domain |

**Requirement 3:**

***All users should be able to logon to ATEConsult’s resources except he Domain Controller’s. Only IT Support staff and Domain Administrators can log onto the server locally.***

In order to long on to the server locally the IT Support Staff and Domain Administrators we need to do “Default Domain Controller GPO” and add those two user groups to “Allow Logon Locally” and all we have to do by using the path below:

Computer Configuration

Policies

Windows Settings

Security Settings

Local Policies

User Rights Management

**Requirement 4:**

***For security reasons, all users must use complex passwords (i.e.at least 10characters) when logging on the network.***

To make the logging password complex we need edit “Default Domain Policy setting” and follow the steps below:

Computer Configuration

Policies

Windows Settings

Security Settings

Account Policies

Password Policy

After that we need to Double-Click on maximum password length and set it to 10.

**Requirement 5:**

***All users, except the IT Support staff, should not be able to access Control Panel or edit the registry settings on Windows.***

By creating a policy named as “Control Panel Policy” in the design and we need to create that in any OU except the IT Support staff. To remove Control Panel from all the OU’s except the IT Support staff OU we need to work as the following steps:

User Configuration

Policies

Administrative

Template

Control Panel

Double-click on “Prohibit access to the Control Panel and PC settings”.

Select enabled to enable restriction.

After that, we need to link the rest of the OU’s to this policy except the IT Support staff. Again, we need to create another policy named as “Registry Editing” in the design and link the rest of the OU’s to this policy except the IT Support staff.

**Requirement 6:**

***Shared folders are maintained in the file server. Two folders “ConsultantSharedDocs” and “SupportStaffDocs” needs to be maintained where Consultants and General Support staff members have read and write access to the folders respectively. Also, the shared folders must be mapped as network drives to be easily accessible for users when they log in.***

To do the following requirement we need to give “Read and Write” access both of the documents. Describing that in the table below:

|  |  |  |
| --- | --- | --- |
| Groups | Folder | Authority |
| ConsultantsAuthority | ConsultantSharedDocs | Read and Write |
| GeneralAuthority |
| ConsultantsAuthority | SupportStaffDocs | Read and Write |
| GeneralAuthority |

Drive Mapping:

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Locations | Drive letter | Authority |
| Create | [\\ATEConsultantServer\Consultant](file:///\\ATEConsultantServer\Consultant)SharedDocs | T | Show |
| Create | [\\ATEConsultantServer\](file:///\\ATEConsultantServer\Consultant)SupportStaffDocs | S | Show |

**Requirement 7:**

***Team Leaders has permissions of all resources of staff and customers except IT Support staff (i.e. C******onsultants, Customers and General Support staff).***

We have to do the following steps to do the requirement:

Group

Member

Add Member

Select TeamLeader User Group

Apply

We have to do the following steps in consultants, Customers and General Support staff except the IT Support Staff.

**Requirement 8:**

***The IT Support Staff are able to manage user accounts and reset passwords for Team Leaders, Consultants, Clients and General Support Staff***

Delegating/Provide control to IT Support Staff Users over Team Leader OU, Consultants OU, Customers/Clients OU and General Support Staff OU with appropriate permissions to manage user accounts and reset passwords.