Self-service user provisioning is currently enabled in this instance, however users with a dot character in their email address may face service disruption, we are testing a fix at present and request you raise a support request for access in these cases while this is being resolved.

ESRI ArcGIS Technical Architecture Plan (TAP)

Created by Hardy, Bryan, last modified by Kamdem, Arnold on Nov 22, 2022

ARCGIS_ENTERPRISEv1.1.vsdx

Effective Date	7/21/2022
Last Revised	11/22/2022
Document Contact	@Kamdem, Arnold @Krishnamoorthy, Badreenarayan
Document Description	ARCGIS ENTERPRISE GEOSPACIAL PROJECT

Table of Contents

Overview

Purpose	*Describe why the document exists*
Description	
Intended Audience	

Project Description

Provide a description of the solution being deployed, how it will be used, who will use it, a general high-level description of the components involved, etc. The goal of the description is to give readers a general idea of what is being built and how it will be used.

Project Links

System	ID	Link
ATOP	ATOP-2861	ATOP-2861 - GIS COE (ESRI) REALIZE
DevOps		Project-Geospatial Stories Board - Boards (azure.com)

Stakeholders

Role	Name	Contact
Business Owner		
Application Owner		
Application Development		
ATO Project Manager		
ATO Architect		
DSG SRM		
DSG Security Architect		

Architecture Diagrams

Logical Architecture

Logical architecture describes how a solution works in terms of function and logical information. From an abstraction level viewpoint, it represents a middle ground, sitting between the Conceptual and Physical architectures. Unlike these, however, logical architecture is quite broad in scope. In fact it allows architects to model things both at a high and low levels, depending on the requirements, which makes it very important for the architecture process. For instance, a diagram that leans strongly towards the conceptual side will be more passive and therefore indicative of connectivity, whereas one that is closer to the Physical level will necessarily be more dynamic and better illustrate sequence.

Instructions
Provide the designed Logical Architecture Diagram along with the detailed write up. This will mainly provide the stakeholders an insight into the expected solution architecture and provide the Cloud Ops architect a perspective into what Azure components can substitute the already existing components in the Logical Architecture Diagram. Include the technical details listed below in addition to any other content:

- Purpose and overview of the architecture
- System definitions that will be a part of the architecture
- Data flow diagram including baseline data flow expectations in the application
- Third party application used in the architecture and respective licensing details
- Validations definition
- Accessibility requirements of the system
- Interfacing requirements
- SLA details
- High Availability requirements
- Data Classifications
- Security requirements

Add logical architecture here. An example is provided below.

https://lucid.app/lucidchart/8e3013ed-36e4-48af-9132-bbdcf66702ff/edit?invitationId=inv_2274deff-b513-4c0d-ab67-6730a875bb3d&page=JsVPdv8go859W#

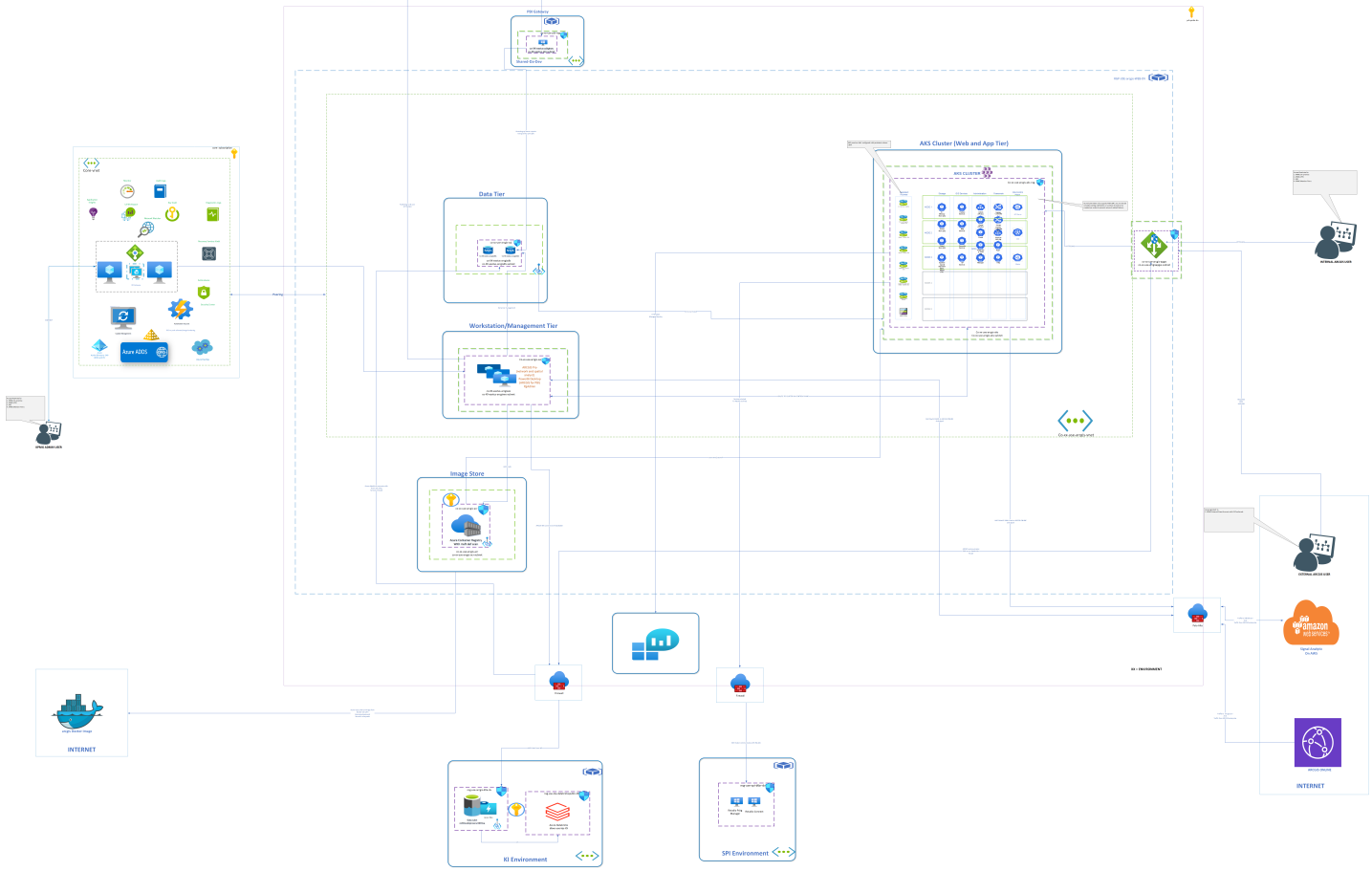
Physical Architecture

This is the lowest level of abstraction, so it is very detail oriented. It includes specific products, data representations, and other technical notions. The purpose of designing the physical architecture diagram is to enable the real life implementation of a specific technology solution. It acts as a guide for the team actually putting the system together. Thorough end-to-end solution architecture addressing all domain inputs (Business, Data, Application, and Infrastructure) provides a useful roadmap for stakeholders and enables dependencies, risks and budget issues to be identified as early as the concept phase. It can take some effort and the right people to get this done, but allocating appropriate time in the beginning offers a better payoff later on when the team has a solid case for the project and delivery is planned well. The physical architecture diagram will be built as a collaborative effort between Cloud Ops and the business as a part of the Define and Develop phases of the overall project with specific time dedicated to create this artifact. Without the physical architecture it is difficult to get an understanding of what we are trying to build and without that understanding it is not possible to automate the build effectively.

To browse through some of the reference architectures and architecture guidelines from Microsoft, refer Reference material from Microsoft.

Instructions
This section should include, in addition to the content listed in the logical architecture, the details related to data transfer between different services, different hardware requirements and the Azure services that will be plugged into the application.

Add physical architecture here. An example is provided below.

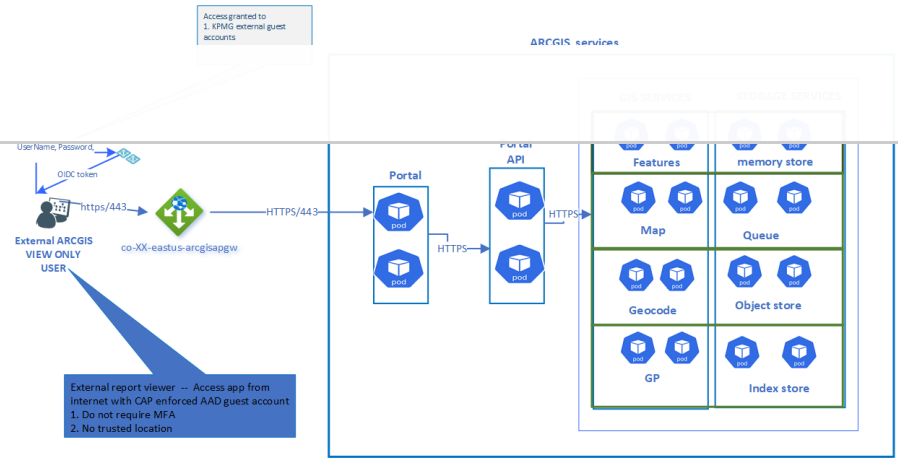


Data Flow

Diagram

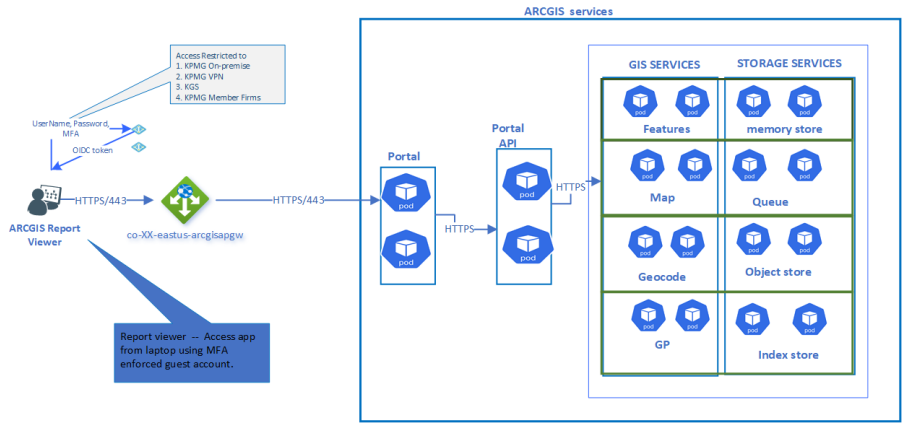
Provide details around the flow of data using a process flow diagram. An example is provided below for reference.

EXTERNAL VIEW ONLY ARCGIS USER ACCESSES ARCGIS SERVICES



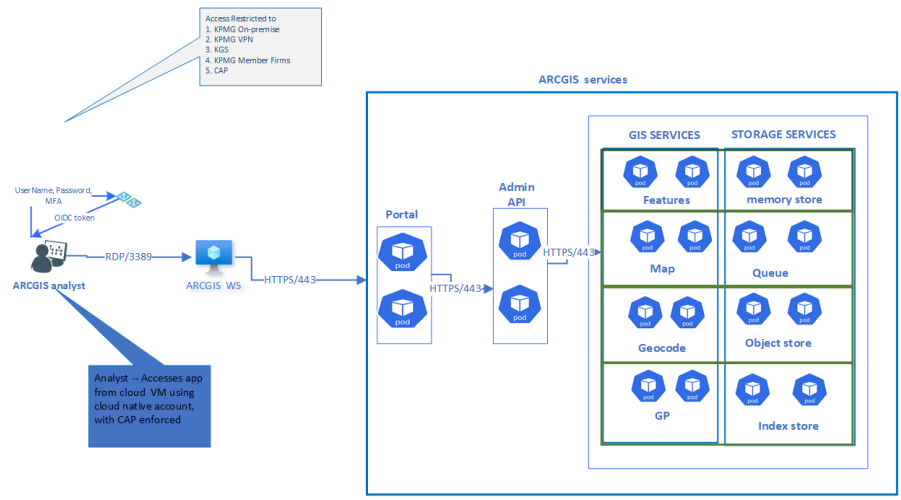
- ARCGIS external viewer connects to the application via application gatewway over https/443.
- ARCGIS external viewers accesses app from laptop using @kpmg.com MFA enforced guest account.
- CAP is not enforced
  1. Do not require MFA
  2. No trusted location enforced

INTERNAL ARCGIS REPORT VIEWER ACCESSES ARCGIS SERVICES



- ARCGIS users connects to application via application gatewway over https/443.
- ARCGIS report viewers accesses app from laptop using @kpmg.com MFA enforced guest account.

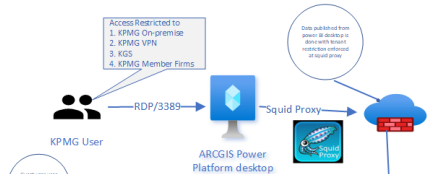
INTERNAL ARCGIS ANALYST ACCESSES ARCGIS SERVICES



Process

- ARCGIS analyst will RDP into cloud vm from their laptops to access enterprise portal using cloud native AADMFA enforced guest account. AAD CAP will be applied to prevent GIS analyst from accessing portal from their laptop.
- CAP policy enforced
  1. Must log in from trusted location

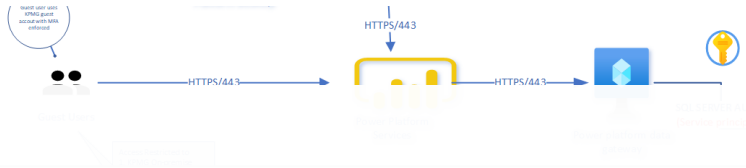
KPMG AND GUEST



Process

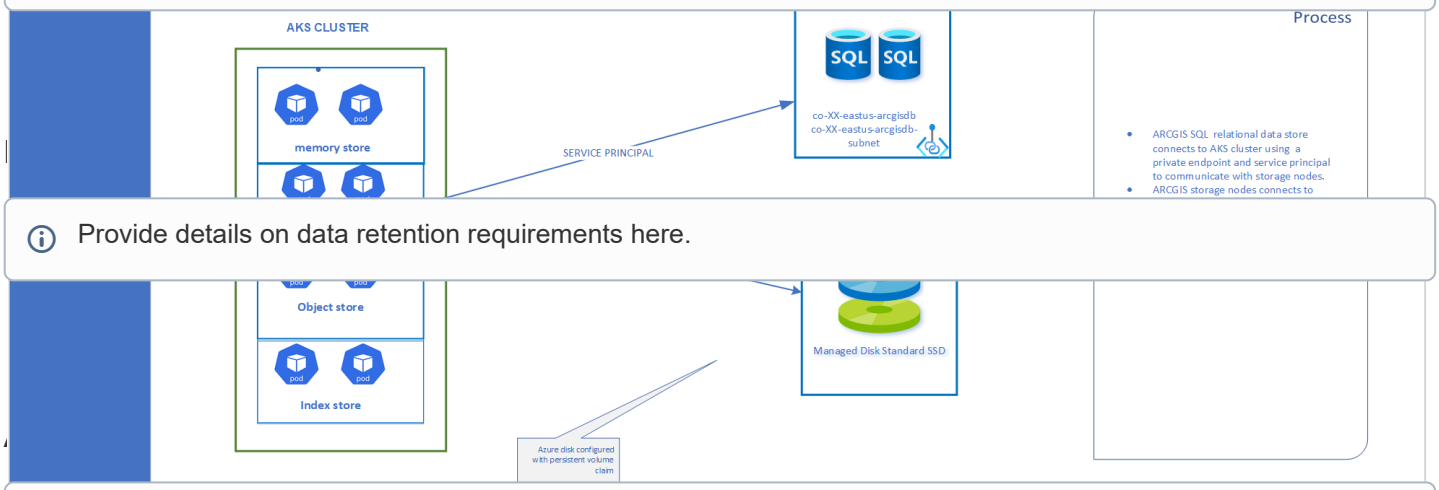
- ARCGIS user publishes data to powerbi via power platform desktop over https (with tenant restriction applied at squid proxy), via the azure firewall.
- Power platform data gateway connects to azure sql with sql auth to securely report data to powerbi for visualization over https.

USER ACCESS POWER BI REPORTS



- Guest user authenticates with MFA enforced guest AAD credentials to access powerbi to view published data via https/443.
- We are planning to upgrade the current

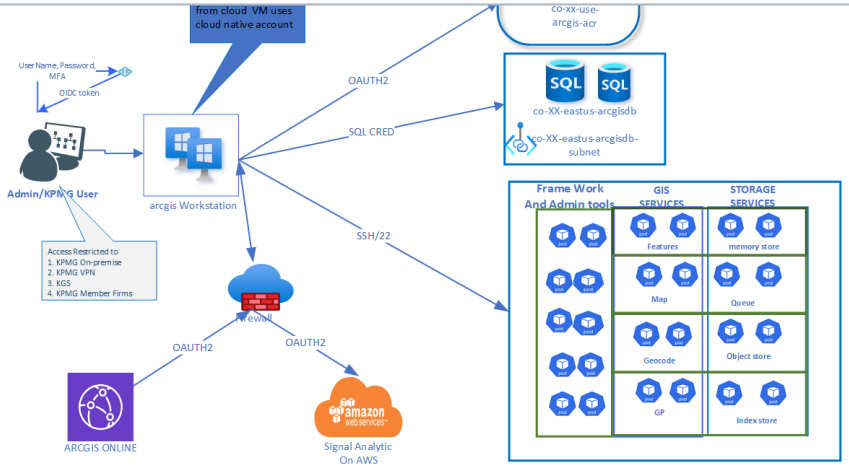
Provide a detailed written outline of the data flow. This may be best delivered via an ordered bullet list of steps in the data flow.



Provide details on data retention requirements here.

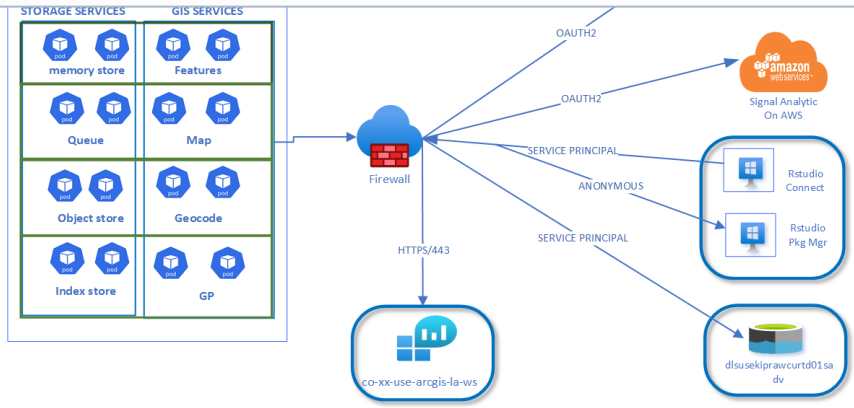
Provide details and diagrams for user authentication flow, as well as the authentication of components and Azure resources that communicate with each other.

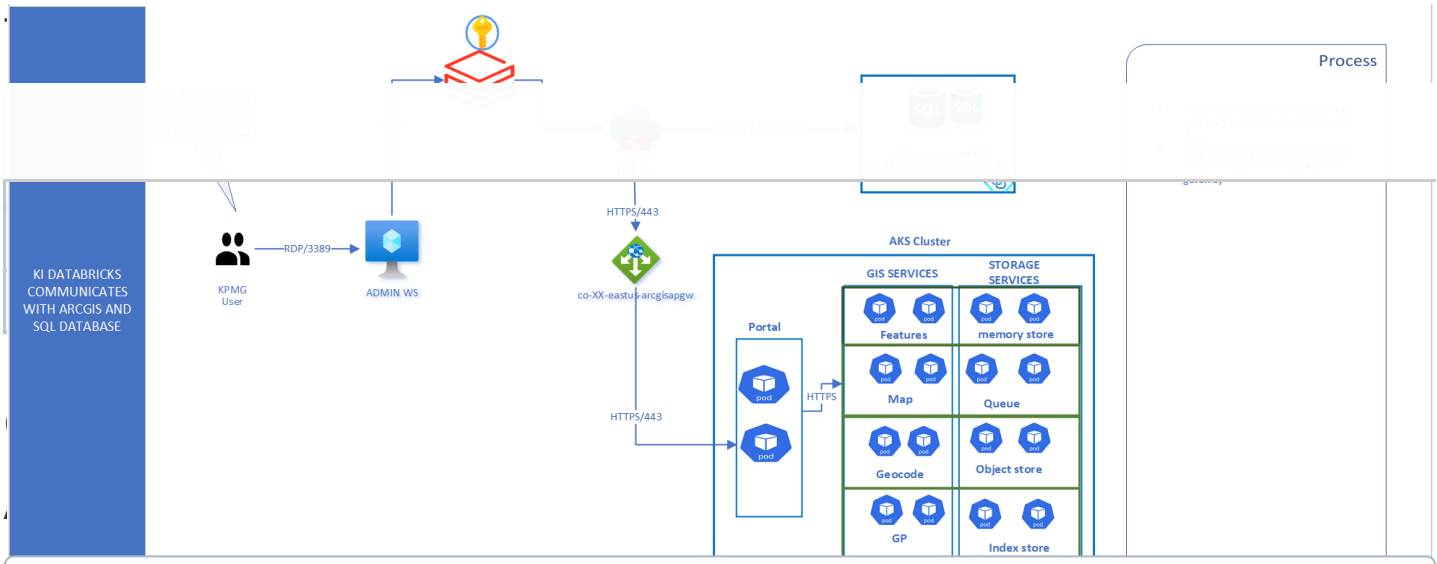
ARCGIS PRO CONNECTS TO ARCGIS RESOURCES



Include details of all APIs that will be consumed by this solution. Include the authentication method used for the API, the endpoint that will be connected to, and a link to the specifications for the API.

ARCGIS ENTERPRISE API COMMUNICATES WITH OTHER EVIRONMENT





Include a list of all existing Azure resources that will be referenced during creation or deployment of this solution. This may include, for example, Azure Active Directory and existing subscriptions, DNS zones, vnets, etc.

The following are existing Azure resources within the environment that will be utilized or consumed in the deployment of this application.

Resource Type	Resource Name	Description

Azure Resources Created

Include a list of all Azure resources that will be created during deployment of this solution.

The following Azure resources will be created during deployment of this application.

Resource Type	Resource Name	Description

Subnets

List all subnets that must be created for this solution. Include the subnet name, CIDR range, and any details on what the subnet will be used for.

Subnet Name	CIDR Range	Notes

Network Security Groups

List all Network Security Groups that will be created for this solution. Include the NSG name, subnet(s) that the NSG will be associated with, and all inbound and outbound rules with related ports, protocols, source/destination, and actions.

NSG Name	Subnet	Rules

Direction	Port	Protocol	Source	Destination	Action	Notes
Inbound						
Outbound						

Firewall Rules

List all firewall rules that must be created for this solution. Include the rule type (network, application / fqdn, etc.), source, destination, protocol, port, and a description justifying the need for each rule.

The following firewall rules must be created on the Azure Firewall in the core subscription.

Rule Type	Source	Destination	Protocol	Destination Port	Description

Public DNS Records

The following DNS entries must be created on the public Azure DNS zone in the core subscription.

Name	Type	TTL	Value	Alias Resource Type	Alias Target

Private DNS Records

The following DNS entries must be created in their corresponding private Azure DNS zones.

Name	Type	TTL	Value	Alias Resource Type	Alias Target

Monitoring

Platform Monitoring

Instructions
Provide component details as listed below:

- Azure Active Directory
  - AAD logins are monitored via Azure Security Center
  - Azure Security Center forward the logs to Splunk Cloud
  - CSIRT has runbook and escalation procedures for AAD login failures
- Component #2
  - Details
  - Details

Workload Monitoring

Instructions
Provide application component details as listed below:

- Application Component #1
  - Details
  - Details
- Application Component #2
  - Details
  - Details

Backup & Recovery

Include any items required for Data backup and recovery configuration including items such as SQL Server retention periods, recovery service vaults, backup policies, etc.

DevOps Configuration

Include all details on DevOps pipelines that must be created as part of this build.

Validation Criteria

List all tests that should be performed by Engineering to validate correct functioning of the underlying infrastructure after build/deployment.

Required Documentation

List all documentation that should be generated during engineering build to meet control requirements and/or facilitate hand-off to Operations team.

Attachments

Attach all files related to this template in this section. If you upload the same document with the same name, Confluence will automatically keep a record of all versions for you.

File	Locked By	Modified
image2020-10-30_15-57-58.png		Oct 27, 2022 by Hardy, Bryan
image2020-4-21_10-31-24.png		Oct 27, 2022 by Hardy, Bryan
ARCGIS_ENTERPRISE.vsdx		Nov 03, 2022 by Kamdem, Arnold
ARCGIS_ENTERPRIS.DFE.png		Nov 08, 2022 by Kamdem, Arnold
ARCGIS_ENTERPRISEv1.1.png		Nov 18, 2022 by Kamdem, Arnold
ARCGIS_ENTERPRISEv1.1.vsdx		Nov 22, 2022 by Kamdem, Arnold
ARCGIS_ENTERPRISE.png		Nov 22, 2022 by Kamdem, Arnold

Drag and drop to upload or browse for files

Download All | Lock All | Unlock All

Related Documents

Provide links to related document on Confluence as a bulleted list in this section. You can easily link existing pages by typing an open square bracket (e.g. [ ) and typing the name of the page you want to link. A list of pages

will automatically appears that you can select from.

Revision History

Be sure to add a new line item to the revision history for all major changes to this document.

Revised On	Version	Revision Description	Revised By

No labels