VIZOR

SECURITY TOPICS

OVERVIEW

There are several topics around security in VIZOR.

For example,

- Security and access control to authorized data in VIZOR
- Security and access control to authorized features in VIZOR
- Authentication to log in to VIZOR
- Secured sessions while using the VIZOR application
- Security and access control to external resources using VIZOR

VIZOR has many security controls in place to allow only authorized staff and users to view, open, modify, authorize and in general work with data based on their role.

VIZOR's security enables managing user access per **data** (assets, purchases, incidents, etc.) and per **feature** (be able to add a new asset, delete an asset, etc.). It is based on user groups, which can be linked to Active Directory or Azure AD security groups.

Users can be created within VIZOR or imported/synchronized with an external system, such as Active Directory. When the users originate in an external system, you can also define what VIZOR group the members of an external group are imported into in VIZOR.

USER GROUPS

Each user is a member of one or more groups. Access to Vizor features and projects is based on group membership. You can enable and disable features and projects on a group-by-group basis. A user can only access a feature or project if the user is a member of a group where the feature or project is enabled.

To control access to VIZOR features, you assign users to the groups based on their roles and responsibilities in the process. For example, a help desk group leader or analyst who is also responsible for administering VIZOR must be a member of the **Admins** group.

SECURITY AND ACCESS CONTROL TO AUTHORIZED DATA IN VIZOR

Use the Web View Editor to set the group access permissions that control who can log on to the Web views of a VIZOR project.

CONTROLLING ACCESS AND SECURITY OF A FIELD

VIZOR has multiple ways to control access to your data. Since data is mostly stored in fields, controlling access and security of a field is paramount.

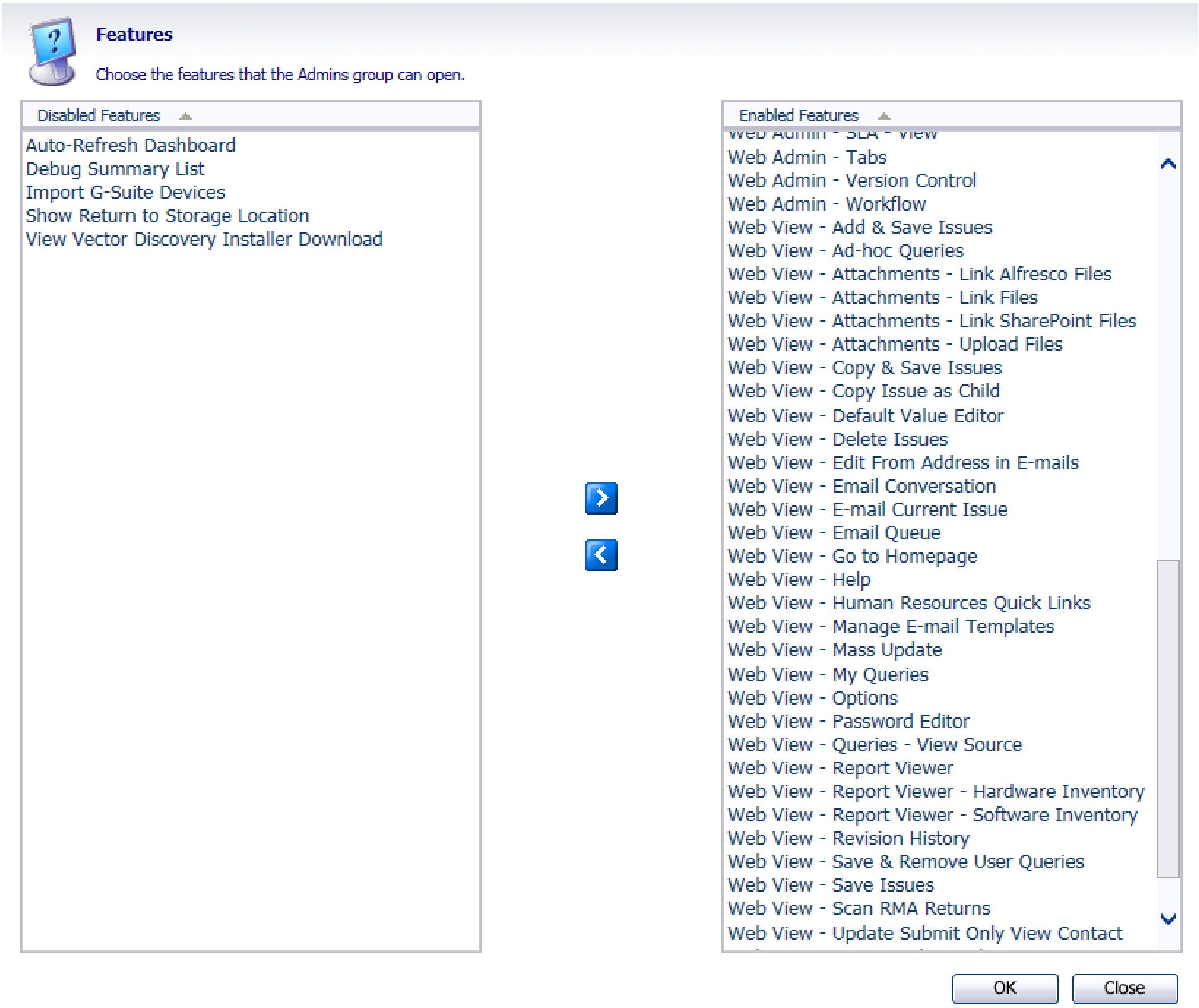
Methods to control access and security of a field:

- Visible or Hidden, in the Field Editor
- Disabled or Read-only, in the Field Editor
- Read-only for specific user groups, in the Field Editor
- Visible or Hidden per Web View, in the Web View Editor
- Read-only per Web View, in the Web View Editor
- Visible or Hidden under custom conditions, using the Business Rule Worfklow Editor
- Read-only under custom conditions, using the Business Rule Worfklow Editor
- Create custom macros using scripting programming language to reflect unique or complex conditions.
- Because access to Web views can be controlled per user group, and you can create any number of Web views, you can combine all these to defined eseentially any possible security, access or authorization situation.

SECURITY AND ACCESS CONTROL TO AUTHORIZED FEATURES IN VIZOR

The main mechanism to authorize users to use features in VIZOR is via the VIZOR Features. Features allow users to create new assets or delete assets, for example.

The following is an example of all the features that a user can be granted access/authorization to:



Features

Choose the features that the Admins group can open.

Disabled Features

- Auto-Refresh Dashboard
- Debug Summary List
- Import G-Suite Devices
- Show Return to Storage Location
- View Vector Discovery Installer Download

Enabled Features

- Web Admin - SLA - View
- Web Admin - Tabs
- Web Admin - Version Control
- Web Admin - Workflow
- Web View - Add & Save Issues
- Web View - Ad-hoc Queries
- Web View - Attachments - Link Alfresco Files
- Web View - Attachments - Link Files
- Web View - Attachments - Link SharePoint Files
- Web View - Attachments - Upload Files
- Web View - Copy & Save Issues
- Web View - Copy Issue as Child
- Web View - Default Value Editor
- Web View - Delete Issues
- Web View - Edit From Address in E-mails
- Web View - Email Conversation
- Web View - E-mail Current Issue
- Web View - Email Queue
- Web View - Go to Homepage
- Web View - Help
- Web View - Human Resources Quick Links
- Web View - Manage E-mail Templates
- Web View - Mass Update
- Web View - My Queries
- Web View - Options
- Web View - Password Editor
- Web View - Queries - View Source
- Web View - Report Viewer
- Web View - Report Viewer - Hardware Inventory
- Web View - Report Viewer - Software Inventory
- Web View - Revision History
- Web View - Save & Remove User Queries
- Web View - Save Issues
- Web View - Scan RMA Returns
- Web View - Update Submit Only View Contact

AUTHENTICATION TO LOG IN TO VIZOR

Users can log into VIZOR using accounts from the following authentication types:

- Vizor user accounts.
- Active Directory user accounts.
- Azure / Microsoft user accounts.
- Windows user accounts.

For the last 3, your users can authenticate using SSO (Single-Sign On), that is, your users never need to log on to VIZOR with their Windows or Network/Active Directory accounts again if the Web browser or Windows is already logged

.

SECURED SESSIONS WHILE USING THE VIZOR APPLICATION

VIZOR sessions via the browser communicate to the Web Server using the HTTP/HTTPS protocol.

By default, HTTPS is used and recommended, which ensures communication between the VIZOR Web and the server is secure and encrypted.

SECURITY AND ACCESS CONTROL TO EXTERNAL RESOURCES USING VIZOR

You can control access and authorization of users to a 3rd party, external system via the Request Portal and custom VIZOR Actions. These VIZOR Actions interact with the external system and grant or remove access to features depending on the configuration.

ACTIVE DIRECTORY ACTIONS

VIZOR can also control security aspects of your network or external systems via the AD connector. The following actions can be automated via the native AD adapter.

- Add user to Security Group
- Assign user to OU
- Change user password
- Create user account
- Delete user account
- Disable user account
- Enable user account
- Remove user from Security Group
- Reset user password

VECTOR DISCOVERY

This section only applies to customers using the Vector Discovery, not when integrating with Microsoft SCCM, LanSweeper, SolarWinds, etc.

The Vector Discovery Server (a.k.a. Vector Asset Manager) communicates with regular Vector Discovery Clients using the HTTP protocol. The server uses IIS for both receiving and sending requests to and from the client.

IP PORTS

By default, this communication occurs over port 443 (for https) but it can be configured to use any port designated by the organization.

SERVER-SIDE PROCESS

Once the information is sent to the server (offline or caching area), the data is parsed and converted into information that is then added to the SQL Server database. This process is performed by the Vector Scheduler Windows Service, which runs under a Windows account designated during installation, which must have read/write permissions to the Offline Area, and SQL access to the database.

ACCESS CONTROL

Access to the information is from Vizor, usually via the Web UI.

Vizor users belong to User Groups which give them different profiles or security roles. Accounts can also be integrated with Windows AD domain accounts, individually per user or via mapping AD Security Groups or OUs to Vizor Groups (roles).

This architecture gives powerful and comprehensive control on access to the data to different users. Vizor can be configured to limit access to individual users to specific computers or groups of computers, specific fields per device, the ability to make certain changes to the device information, etc.

By default, Vizor includes the following user Groups or roles:

Role (user group)	Access to Views
Software Managers	Software Licenses Agreements & Purchases Employees My Actions
IT Asset Managers	Assets Employees Locations Agreements & Purchases My Actions Roles & Policies
IT Managers	Assets Software Licenses Employees Locations Agreements & Purchases My Actions Roles & Policies Approve Change Requests Help Desk Incidents
Employees	Request Assets Search KB Submit a HelpDesk Ticket
Helpdesk Analyst	Help Desk Incidents & Problems Change Requests Search KB
HR Manager	New Employee Onboard Batch Onboard

	Terminate Employees Employees Locations Roles & Policies
Release Manager	Release Management

CLIENT DEPLOYMENT

Administrator privileges are required to install the Vector Client, but not to run the client on a regular basis (see Windows Account).

Vector provides tools to push the client to be installed remotely, however, a number of security conditions need to be met in order for this to be successful (Admin$ share, local administrative permissions for the client push installer account, etc.).

For most environments, those where computers belong to an AD domain, Group Policy client installation and software update-based client installation methods offer a secure and simple method of installation.

Including the Vector Client as part of the Computer OS image is also a secure way, provided you have access controls on the person who performs the installation/deployment of the OS.

WINDOWS ACCOUNT ON CLIENTS

By default, the Vector Discovery Client runs as a Windows Service. The service is called Vector Asset Management Agent and it is run using the Local System account by default. No additional Windows User Account is needed; however, it is possible to run the service with a different Windows user, ostensibly created solely for the Vector Discovery function. Keep in mind that if the user is changed, the user must have elevated privileges, and essentially be a local administrator, plus it needs to be valid in the computers where the client runs and a domain user account may not be valid for computers outside the LAN.

INTERNET – DEPLOYMENT OUTSIDE THE ORGANIZATION'S NETWORK

The Vector Discovery Client can be installed on a computer outside the organization's LAN or WAN.

When the Vector Discovery Client is outside the network, the client communicates with the server(s) via the Internet.

In this environment, it is highly recommended to protect the Vector Discovery (a.k.a. Vector Asset Manager) Server behind a firewall and use TSL/SSL (https protocol) for the communication between the client and the server. The server can be in a DMZ network or the LAN.

The firewall should be configured to use the designated port (80, 443, etc.) and it can be restricted to permit only inbound connections started from the outside.

For increased security when exchanging information between the client and server, an encrypted security key is used which is unique to the site, and can be modified by the server.

In addition, you can also use public key infrastructure certificates for client communications. In this case, the IIS where the Vector server runs must be configured for HTTPS only and deploy the certificates to the clients. It is also possible to add SHA-256 signature or fingerprint.