MVP 10.2 Security Overview

MarkVision Professional 10.2 uses several new features that provide more comprehensive security for your network devices from unauthorized use in the forms of User Authentication and Device Protection.

MVP 10.2 approaches security in terms of both controlling access to the MarkVision application (User Authentication) as well as providing greater control over access to specific network devices and device features (Device Password Protection).

Here are some of the new security features that MarkVision Professional 10.2 has to offer:

- LDAP Server Authentication including secure SSL login
- Active session expiration
- Account password expiration
- Adapter password conformance

User Authentication

User authentication incorporates each of the security features that verify user access to the MarkVision application and its various tasks. The most prominent feature of User Authentication is LDAP Server Authentication.

LDAP Server Authentication

LDAP Server Authentication provides administrators with the ability to assimilate corporate login IDs and passwords for use with MarkVision Professional. By using LDAP authentication, MVP can now connect to LDAP servers that utilize the Microsoft Active Directory service to authenticate a user's login. The option to authenticate user IDs through an LDAP server eliminates the need to use a unique user ID and password when accessing MarkVision Professional. As a result, in addition to reducing the amount of upkeep user accounts require by MVP administrators, MarkVision is more holistically integrated into your existing security framework.

If LDAP Server Authentication has been implemented, when a user logs into MVP, they will enter the user ID and password that they use for their company's local network in place of a standard MarkVision login. The MarkVision Server then accesses the directory service on your company's LDAP server and authenticates the user's login through one of two authentication mechanisms: either a simple bind protected by SSL, or a secure bind using Kerberos.

If you choose to use simple LDAP authentication, you may need to set up an MVP Server account on your LDAP server. Also, when using simple LDAP authentication, if you want to utilize SSL, you need to select the SSL checkbox, and select the appropriate SSL certificate from the store to complete the setup.

If you use Kerberos (secure) LDAP authentication, the need to set up an MVP Server account will be determined by your current Kerberos configuration. For information on determining if you need to set up an MVP Server account for Kerberos, see your Kerberos documentation. Character limitations and the number of available login attempts may differ between servers. As a result, it is important to ensure that you understand the specific limitations of your Kerberos server's configuration.

NOTE: If you are using Kerberos validation with MVP, the Kerberos server must reside on the same computer as your LDAP server for MVP to work.

MarkVision™ Professional

To enable LDAP Server authentication

LDAP Server authentication is only accessible through the Master Administrator account. If you are upgrading from a previous version of MarkVision Professional, open the User Accounts and Groups task under the MarkVision menu, or select User Accounts and Groups from the All Tasks list. Select the administrator account, and click **Edit**.

When installing MarkVision Professional for the first time, you will have the option to set up LDAP Server authentication while creating the Master Administrator account.

LDAP authentication works for all user accounts with the exception of the Master Administrator account. As a result, the administrator will still need to maintain an MVP Master Administrator account with a unique user ID and password that is saved on the MarkVision Server. Make sure that the administrator password is defined before proceeding with LDAP Server authentication setup, as MVP requires that at least an administrator account be in place before setup can begin.

1 Once you have accessed the Master Administrator account wizard, click the **Authenticate with an LDAP Server** checkbox (see figure 1).

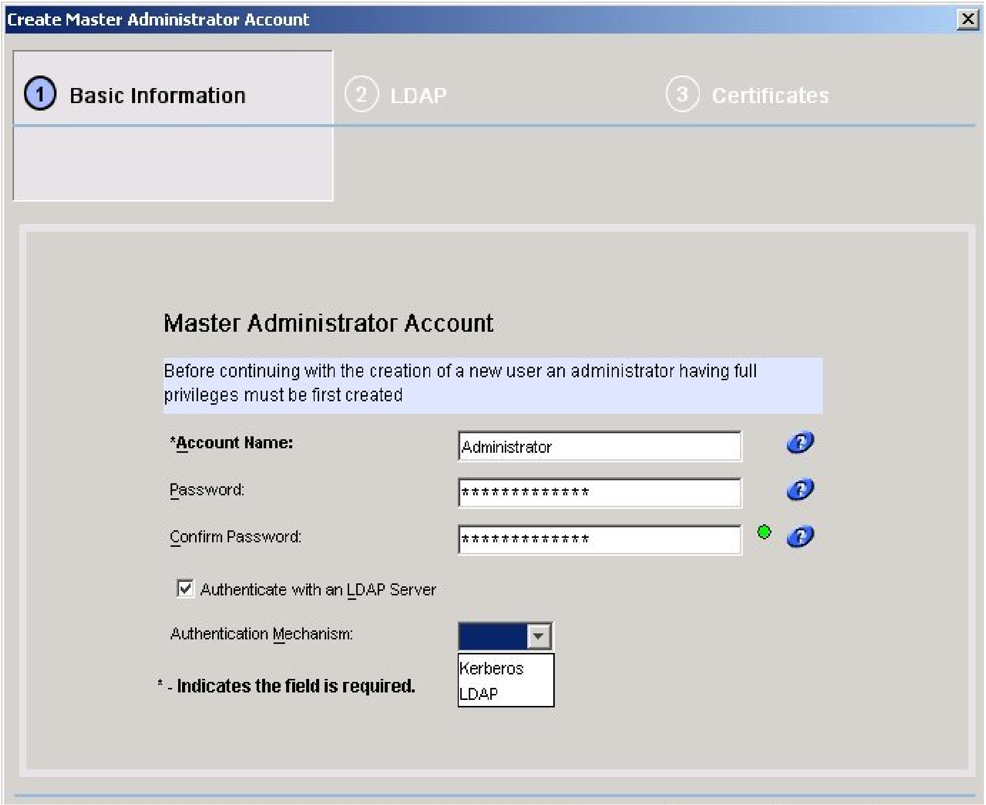
2 Select the authentication mechanism you want to use from the drop-down list. The options are LDAP or Kerberos.

3 Enter your LDAP Server information.

If Kerberos (Secure) is selected as the authentication mechanism, enter the **KDC IP HostName** and **Domain Name** of your LDAP Server under the **Kerberos Configuration** tab.

If LDAP (Simple) is selected as the authentication mechanism, enter your **Server Address**, **Port Number**, **Base Dn**, and **User Attributes** under the **Users** tab.

4 Enter Your MVP Server information under the MVP Server tab. This step is needed only if your LDAP Server



Master Administrator Account

Before continuing with the creation of a new user an administrator having full privileges must be first created

*Account Name: Administrator

Password: **************

Confirm Password: **************

☑ Authenticate with an LDAP Server

Authentication Mechanism:

Kerberos
LDAP

* - Indicates the field is required.

figure 1

configuration requires authentication by the MVP Server.

If you selected Kerberos as the authentication mechanism, in the MVP Server Account area, enter a **User Name** and **Password** that you have previously set on the LDAP Server.

If LDAP is selected as the authentication mechanism, in the MVP Server LDAP Account area, enter a **Distinguished Name** and **Password** that you have previously set up on the LDAP Server.

5 If you selected Kerberos as the authentication mechanism, click **Finish**. If you selected LDAP for a simple bind, go on to the next step.

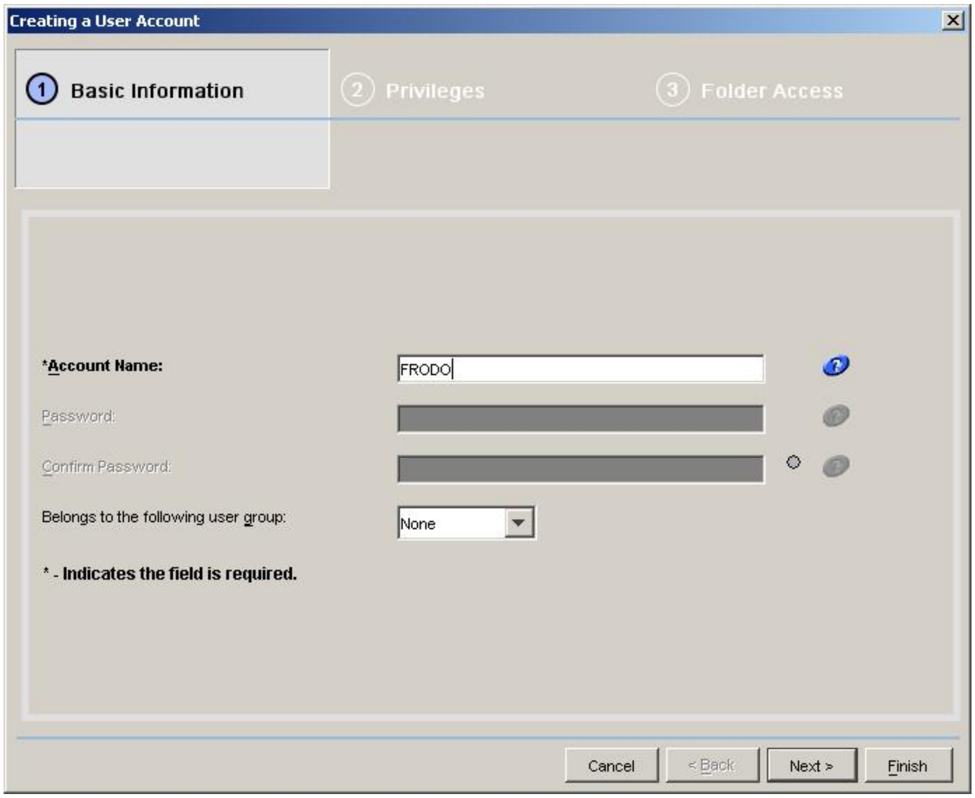
6 If you selected LDAP as the authentication mechanism and want to utilize SSL, click the **Use SSL** checkbox, enter the Certificate Store password, and then click **Next**. If you do not want to use SSL, click **Finish**.

7 Select the appropriate certificate for use with the SSL protocol. Without the proper certificate, the SSL protocol will not work. Your LDAP server should have a facility for issuing a certificate request.

8 Click **Import**.

9 Click **Finish**.

Once LDAP authentication has been implemented, it is no longer necessary to enter individual user account passwords on the MarkVision Server, as each user ID is authenticated with with the LDAP Server. As a result, the User Accounts and User Groups dialog changes accordingly, and the user account password dialog is disabled (see figure 2).



Creating a User Account

*Account Name: FRODO

Password:

Confirm Password:

Belongs to the following user group: None

* - Indicates the field is required.

figure 2

Active Session Expiration

Active Session Expiration is a new feature in MVP 10.2 that controls the amount of time that an MVP client session will remain idle before locking the user out of MarkVision and prompting them to re-enter their user ID and password.

With this feature, a MarkVision Professional administrator will have the option to set a specific interval of time under MVP's Administrative Settings that determines the maximum amount of time that client session can be open and active without any interaction from the user. This helps to prevent unauthorized users from gaining access to unattended MVP clients.

To set the Active Session Expiration interval

1 Go to **MarkVision → Administrative Settings**, or select **Administrative Settings** from the All Tasks list (see figure 3).

2 Under the Intervals section of the dialog, specify the active session expiration interval in minutes (10 to 60 minutes).

3 Click **OK**.

To remove active session expiration, select the **Never** radio button.

Account Password Expiration

Similar to Active Session Expiration, administrators can set the interval of time for which an MVP account password is valid. By forcing MVP users to regularly change their passwords, the Account Password Expiration feature in turn reduces the likelihood that a user password could become compromised.

When implemented, Account Password Expiration applies to all user accounts with the exception of the master administrator account. This prevents the application from timing out the administrator's password, effectively shutting out all administrative access. As a result, The MVP administrator will be responsible for maintaining the security for their own password.

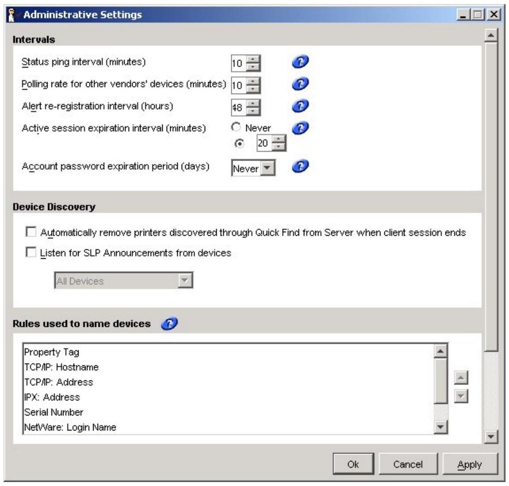
In addition, if LDAP User Authentication is used as the primary security protocol for user IDs and Passwords, Account Password Expiration is disabled within the application, as there is no need to maintain an MVP specific password for use with the user's account.

Once Account Password Expiration is enabled, each MVP user account should be provided access to the **Change Password** task to eliminate the need for an administrator to facilitate a password change for every user account as needed. Because some users may change their passwords at different intervals, and the password expiration interval resets for each password once it is changed, it becomes exponentially more difficult for a single administrator to manage regular password maintenance.

To set the Account Password Expiration interval

1 Go to **MarkVision → Administrative Settings** or select **Administrative Settings** from the All Tasks list (see figure 3).

2 Under the Intervals section of the dialog, specify the account password expiration interval in days. Click **OK**. To remove the password expiration interval, select **Never**.



Administrative Settings

Intervals

Status ping interval (minutes) 10

Polling rate for other vendors' devices (minutes) 10

Alert re-registration interval (hours) 48

Active session expiration interval (minutes) ○ Never ● 20

Account password expiration period (days) Never

Device Discovery

□ Automatically remove printers discovered through Quick Find from Server when client session ends

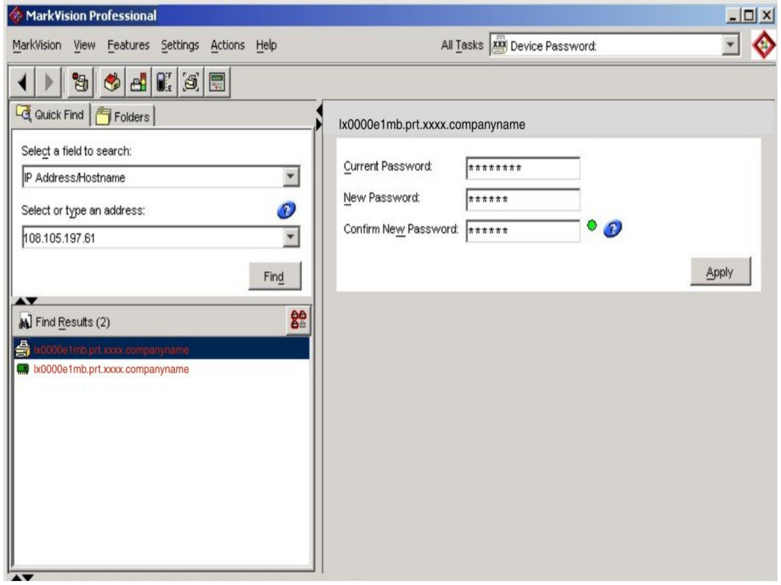
□ Listen for SLP Announcements from devices

All Devices

Rules used to name devices

Property Tag
TCP/IP: Hostname
TCP/IP: Address
IPX: Address
Serial Number
NetWare: Login Name

figure 3



All Tasks: Device Password:

Select a field to search: IP Address/Hostname

Select or type an address: 108.105.197.61

Find Results (2)

- lx0000e1mb.prt.xxxx.companyname
- lx0000e1mb.prt.xxxx.companyname

lx0000e1mb.prt.xxxx.companyname

Current Password: ********

New Password: ******

Confirm New Password: ******

figure 4

Device Password Protection

In addition to the security capabilities of User Authentication, which limit user access to the MarkVision application, MVP 10.2 includes Adapter Password Conformance as a second level of protection for your network devices.

Adapter Password Conformance provides a greater emphasis on the password protection of individual network devices by enforcing the use of device passwords. Through the use of three new tasks, Adapter Password Conformance limits the ability of MarkVision users to access and manipulate network device settings and properties.

The three tasks that make up Adapter password conformance are:

- Enter Device Password
- Device Password
- Manage Global Password List

The Enter Device Password task provides password protected access to specific network devices. When a user attempts to access a password protected device, MarkVision recognizes the device's password and provides a dialog screen prompting the user to enter it. The user is then granted temporary access to the device, lasting only for the duration of the current client session.

Just as devices that are not supported by a specific task are displayed with a black line through the device icon and IP address, devices that are password protected are displayed in red and include floatover text that identifies the device as password protected.

Using the Enter Device Password task

1 Go to **MarkVision → Enter Device Password**, or select Enter Device Password from the All Tasks list (see figure 4).

2 Select the device you want to access from the **Find Results** window.

3 Enter the device password.

4 Click **Apply**.

While the Enter Device Password task lets you access a password protected device, the Device Password task provides an interface to set or change a network device's password. Once a device's password has been set, the device's display in the Find Results window will turn red to indicate that it is now password protected.

Using the Device Password task

1 Go to **Settings → Security → Device Password**, or select **Device Password** from the All Tasks list.

2 Select the device that you want to set or change a password for.

3 Edit the **Password** field accordingly:

- If you want to change an existing device password, enter the device's current password.
- If you want to create a new device password, delete any text in the **Current Password** field and proceed to the next step.

4 Enter the new password in the **New Password** field.

5 Confirm the device password. If the passwords match, the light next to the field will turn green. If the passwords do not match, the light will remain red.

6 Click **Apply**.

To remove a password from a device

1 Go to **Settings → Security → Device Password**, or select **Device Password** from the All Tasks list.

2 Select the device that you want to remove the password from.

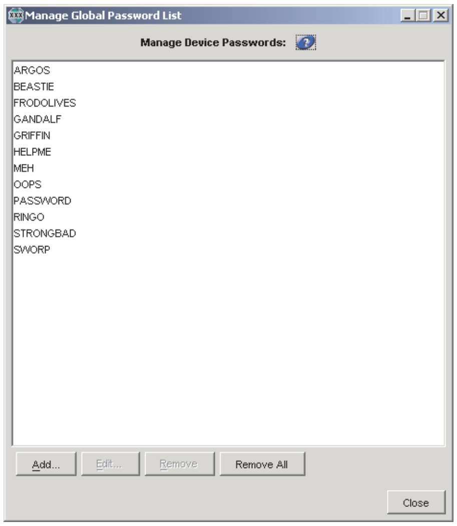
3 Enter the device's current password.

4 Delete any text (including blank spaces) from the **New Password** and **Confirm Password** fields so that both text fields are blank.

5 Click **Apply**.

The Manage Global Password List task allows administrators to perform quick and efficient device management despite increased security. This task lets you create and manage a master list of device passwords. When a user has access to the Manage Global Password List task, if a network device's password is included in the list, the user is provided access to any device that password applies to on the network. As a result, this task should be restricted to administrative personnel only.

Each entered password is displayed in the device password list uppercase. As mentioned previously, for security purposes, because this list displays important device passwords, it is recommended that access to this task be limited to authorized personnel only, and that the task not be left open and on display.



ARGOS
BEASTIE
FRODOLIVES
GANDALF
GRIFFIN
HELPME
MEH
OOPS
PASSWORD
RINGO
STRONGBAD
SWORP

figure 5

To add a device password to the Manage Global Password List

1 Go to **MarkVision → Manage Global Password List**, or select **Manage Global Password List** from the All tasks list.

2 Click **Add** (See figure 5).

3 Enter the new password.

4 Click **OK**.

To edit a device password

1 Go to **MarkVision → Manage Global Password List**, or select **Manage Global Password List** from the All Tasks list.

2 Select the password you want to edit.

3 Click **Edit**.

4 Enter a new password.

5 Confirm the changed password.

6 Click **OK**.

To delete a device password

1 Go to **MarkVision → Manage Global Password List**, or select **Manage Global Password List** from the All Tasks list.

2 Select the password that you want to delete from the list.

3 Click **Remove**.

4 Click **Yes**.

Click **Remove All** to delete all passwords from the list.