Enabling Local Admin Password Management for Windows

In a Windows environment, it is crucial to have a robust password management system in place to ensure the security of local administrator accounts. By enabling local admin password management, administrators can effectively manage and update passwords for these accounts, minimizing the risk of unauthorized access and potential security breaches. This article aims to provide a step-by-step guide on how to enable local admin password management in a Windows environment.

Examples:

1. Using Group Policy:
    - Open the Group Policy Management Console.
    - Navigate to the desired Group Policy Object (GPO) or create a new one.
    - Expand Computer Configuration -> Preferences -> Control Panel Settings -> Local Users and Groups.
    - Right-click on Local Users and Groups and select New -> Local User.
    - Set the desired username and password for the local admin account.
    - Apply the GPO to the appropriate organizational units (OU) or target computers.

2. Using PowerShell:
    - Open PowerShell with administrative privileges.
    - Run the following command to set a new password for the local admin account:

```
Set-LocalUser -Name "Administrator" -Password (ConvertTo-
SecureString -String "NewPassword" -AsPlainText -Force)
```