DATA SHEET

blueprism®
Robotic Process Automation Software

Credential Manager

The Blue Prism Credential Manager provides a number of functions and features for the secure storage of the user credentials which are used to access target applications. By encrypting and storing credentials securely, Blue Prism can log into applications within a secure runtime environment whilst preventing the casual user or developer from re-using those credentials away from the production environment.

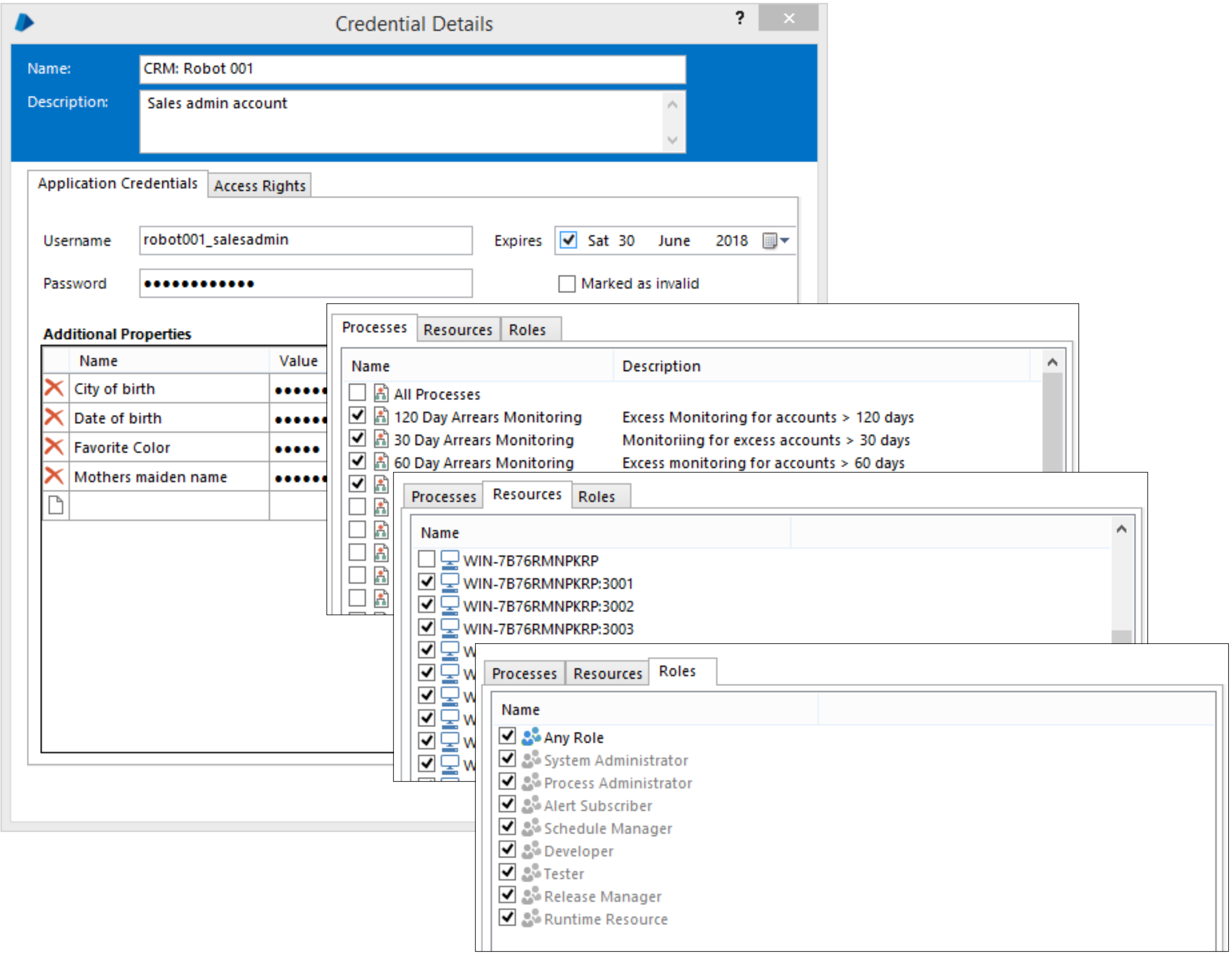
Overview

The Credentials Management functionality provides a secure repository for login details used to access target applications. Credentials are stored in the Blue Prism database, but are encrypted in such a way that only those who are authorized can retrieve them. The encryption key is stored separately, on the Blue Prism Application Server machine, and is used to provide credentials to validated clients.

The Credentials Management system is responsible for determining which processes, Resource PCs and users are able to access this information, and for providing it on request if allowed by a set of permissions controlled via System Manager.

Used in conjunction with Active Directory integration and the Blue Prism server, the Credentials Manager creates a secure and fully audited access control capability for enterprise implementations.

The Credential Manager is only available for Blue Prism Enterprise Editions.



Credential Details

Name: CRM: Robot 001

Description: Sales admin account

Application Credentials | Access Rights

Username: robot001_salesadmin

Expires: ☑ Sat 30 June 2018

Password: ••••••••••••

□ Marked as invalid

Additional Properties

Name	Value
City of birth	••••••
Date of birth	••••••
Favorite Color	•••••
Mothers maiden name	••••••

Processes | Resources | Roles

	Name	Description
□	All Processes	
☑	120 Day Arrears Monitoring	Excess Monitoring for accounts > 120 days
☑	30 Day Arrears Monitoring	Monitoriing for excess accounts > 30 days
☑	60 Day Arrears Monitoring	Excess monitoring for accounts > 60 days

Processes | Resources | Roles

	Name
□	WIN-7B76RMNPKRP
☑	WIN-7B76RMNPKRP:3001
☑	WIN-7B76RMNPKRP:3002
☑	WIN-7B76RMNPKRP:3003

Processes | Resources | Roles

	Name
☑	Any Role
☑	System Administrator
☑	Process Administrator
☑	Alert Subscriber
☑	Schedule Manager
☑	Developer
☑	Tester
☑	Release Manager
☑	Runtime Resource

Authorization

Access to each set of credentials is governed at runtime by the following criteria:

- Process - Only specified processes can retrieve the credentials. Where a credential is used as part of a sub-process or within a Visual Business Object, the parent process (e.g. the one that started the session) must be appropriately authorized. Therefore, if a second process attempted to use a pre-built object; it will be prevented from using the associated credentials unless it is explicitly authorized.
- Resource – Credentials can be restricted such that only specified Runtime Resources are authorized to retrieve and utlize the credentials.
- User Role - Restricts access to the credential based on the account that the Runtime Resource is operating as. This is only valid for Runtime Resources which are NOT public (i.e. /public) and which have been configured to run under the context of a user (i.e. /SSO or /user [username] [password]).
  Restricting access to a credential by User Role will prevent the credential from being accessed in the following scenarios:
  - When process sessions are created by the scheduler.
  - When process sessions are created on Resources which are configured as public.

> It is not appropriate to restrict based on User Role when process sessions are created by the scheduler

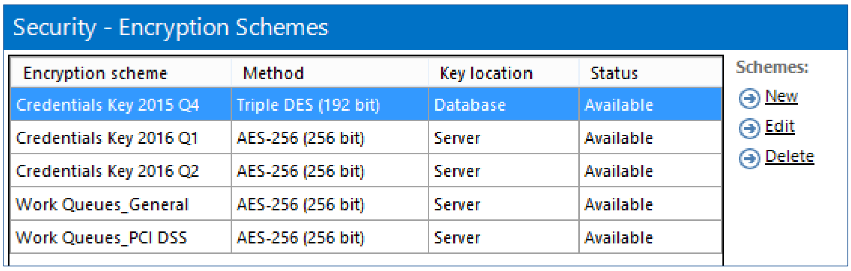
These restrictions work in combination, i.e. if a set of credentials is restricted by Processes and Resource then both of these criteria must be fulfilled to allow the credentials to be retrieved.

At the request of an authorized and validated client, a credential is decrypted locally on the Blue Prism Server and passed to that client via a secure connection.

Recommended configuration

It is recommended that the configuration of the Blue Prism environment will include:

- Encryption Schemes configured with a Server key location.
- Configuring Application Servers to store the keys within separate files and optionally applying custom security to the files to restrict access to only the Blue Prism Server service log on account (and a named administrator).



Security - Encryption Schemes

Encryption scheme	Method	Key location	Status
Credentials Key 2015 Q4	Triple DES (192 bit)	Database	Available
Credentials Key 2016 Q1	AES-256 (256 bit)	Server	Available
Credentials Key 2016 Q2	AES-256 (256 bit)	Server	Available
Work Queues_General	AES-256 (256 bit)	Server	Available
Work Queues_PCI DSS	AES-256 (256 bit)	Server	Available

- Configuring all clients to connect via an Application Server, and to establish secure connections.
- Leveraging Single Sign On for Blue Prism.
- Ensuring an encrypted communication channel between Application Servers and the database.

Where Application Servers are not used within the environment, or where native communication security cannot be applied, it may be necessary to manually configure external security measures to prevent sensitive information being transmitted as plain-text.

Data Security

Algorithm and Key Location

There are a number of encryption algorithms available which can be used to protect credentials and encrypted work queue information.

Name	Key length	Notes	Key generation information
AES-256 AesCryptoService (5.0.24+)	256 bit	Default implementation leveraging CBC	Blue Prism can be configured to use a manually generated key; or users can use the Generate Key functionality within Blue Prism. Keys generated within Blue Prism are created using RNGCryptoServiceProvider which provides a cryptographically strong sequence of random values.
AES-256 RijndaelManaged	256 bit	Default implementation leveraging CBC	
3DES	192 bit	CBC mode with keying option 1	

Protecting the key

When configuring an encryption scheme it is possible to select whether the key will be stored:

- **Database:** the encryption key will be stored within the Blue Prism database. This is commonly appropriate for scenarios where there isn't an Application Server deployed.
  Supports clients that connect directly to the database, and those that connect via an Application Server.
- **Blue Prism Server** (recommended): the encryption key will be stored on the Application Server – in this situation the key will need to be manually deployed to each Application Server within the enviroment. This is the most commonly selected scenario as it ensures the key is stored separately to the encrypted data.
  Supports clients that connect via an Application Server.

> When selecting to store the key on the Application Server it can be stored within the Blue Prism configuration file, or within a separate Blue Prism managed file. By selecting to use a separate file it is possible to add custom controls such as by applying EFS to restrict access.
>
> If restricting access it is necessary as a minimum to ensure access is provided to the Blue Prism Server service account.

Data Encryption/Decryption

When a client device submits data that needs to be stored using reversible encryption, or requests data that is stored using reversible encryption, the device that is responsible for carrying out the conversion between plain-text and cipher-text will be dependent on how the client device is connected to the environment.

- **Application server connection** (recommended): The Application Server is responsible for converting between plain-text and cipher-text for client devices that connect via a Blue Prism Application Server.

  When appropriately configured, the plain-text will be transmitted between client and server over a secure channel, and the cipher-text will be trasmitted between the server and the database over a secure channel.
- **Direct database connection** (not recommended): Client devices that have a direct connection to the Blue Prism database will be responsible for requesting the key and locally converting the data item between plain and cipher text.

When appropriately configured the cipher-text and key will be transmitted between the client and database over a secure channel.

Irrespective of where the conversion takes place, once the conversion has taken place the memory on the device is immediately cleared and disposed.

Key revocation

Blue Prism provides the ability easily revoke a key, and there is an option to forcibly revoke (i.e. immediately convert all data encrypted with an old key to use a new key).

The steps required to configure Blue Prism to use a new key for all subsequent data encryption and decryption include:

1. Create a new encryption scheme record.
   Where the key is stored in the database, add the key to the record.
   Where the key is stored on the application server, update the configuration of each application server to hold the key.
2. Update the Credential Manager to use the new scheme
3. Update any applicable Work Queues to use the new scheme
4. Mark the “old” encryption scheme as unavailable

> Data that is encrypted with the previous keys will still be decrypted using those original keys, but when that data is updated it will be re-encrypted with the currently active key(s).
>
> To forcibly update all data encrypted with previous keys the AutomateC.exe command line switch /reencryptdata can be used. (optionally specifying the batch size and maximum interations).
> *[See Product Help for more information]*

Frequently Asked Questions

1. **How is the key passed to the client?**
   At the request of an authorized and validated client, a credential is decrypted on the Blue Prism Server and the plain text result is passed to the client via a secure connection.
   The keys are NOT shared with the client unless they are configured to use a direct database connection (not recommended). In this scenario the key will be shared over a secure channel.
2. **Is it possible to periodically use a new key for data encryption?**
   Yes. An overview of the steps required to configure the platform to use a different key for data encyption are included within the main body of the document.