

**Links to Other API pages:** [Cisco Unity Connection APIs](#)

|   |
|---|
| <b>CUPI Guide Contents</b>                      |
| <a href="#">API Overview</a>                    |
| <a href="#">Index of All CUPI Documentation</a> |

## Contents

- [1 User Password and PIN Settings API](#)
  - ◆ [1.1 Listing User PIN Settings](#)
  - ◆ [1.2 Listing User Password Settings](#)
  - ◆ [1.3 Update Password/PIN Settings](#)
  - ◆ [1.4 Unlock Password/PIN Settings](#)
  - ◆ [1.5 To Unlock Password](#)
  - ◆ [1.6 Change Password/PIN](#)
  - ◆ [1.7 Explanation of Data Fields](#)

## User Password and PIN Settings API

### Listing User PIN Settings

GET https://<Connection-server>/vmrest/users/<user-objectid>/credential/pin

The following is the response from the above \*GET\* request and the actual response will depend upon the information given by you:

```
<Credential>
  <URI>/vmrest/users/9375d893-c8eb-437b-90bf-7de4b1d0c3e8/credential/pin</URI>
  <UserObjectId>9375d893-c8eb-437b-90bf-7de4b1d0c3e8</UserObjectId>
  <CredentialType>4</CredentialType>
  <Credentials/>
  <IsPrimary>>false</IsPrimary>
  <CantChange>>false</CantChange>
  <DoesntExpire>>true</DoesntExpire>
  <TimeChanged>2013-03-05 11:24:33.344</TimeChanged>
  <HackCount>5</HackCount>
  <Locked>>true</Locked>
  <TimeLastHack>2013-03-11 10:23:30.581</TimeLastHack>
  <TimeLockout>2013-03-05 11:24:33.344</TimeLockout>
  <Alias>Texoma</Alias>
  <CredMustChange>>true</CredMustChange>
  <CredentialPolicyObjectId>a97ff291-8e60-475a-b7ee-e956ae83a730</CredentialPolicyObjectId>
  <Hacked>>false</Hacked>
  <ObjectId>3f6f1cb0-3b00-45b5-91fd-d8553737eec7</ObjectId>
  <EncryptionType>3</EncryptionType>
```

## Cisco\_Unity\_Connection\_Provisioning\_Interface\_(CUPI)\_API\_--\_User\_Password\_PIN\_Settings

</Credential>

Response Code: 200

### Listing User Password Settings

GET https://<Connection-server>/vmrest/users/<user-objectid>/credential/password

The following is the response from the above \*GET\* request and the actual response will depend upon the information given by you:

```
<Credential>
  <URI>/vmrest/users/9375d893-c8eb-437b-90bf-7de4b1d0c3e8/credential/password</URI>
  <UserObjectId>9375d893-c8eb-437b-90bf-7de4b1d0c3e8</UserObjectId>
  <CredentialType>3</CredentialType>
  <Credentials/>
  <IsPrimary>>false</IsPrimary>
  <CantChange>>false</CantChange>
  <DoesntExpire>>true</DoesntExpire>
  <TimeChanged>2013-03-05 11:24:33.344</TimeChanged>
  <HackCount>5</HackCount>
  <Locked>>true</Locked>
  <TimeLastHack>2013-03-11 10:23:30.581</TimeLastHack>
  <TimeLockout>2013-03-05 11:24:33.344</TimeLockout>
  <Alias>Texoma</Alias>
  <CredMustChange>>true</CredMustChange>
  <CredentialPolicyObjectId>a97ff291-8e60-475a-b7ee-e956ae83a730</CredentialPolicyObjectId>
  <Hacked>>false</Hacked>
  <ObjectId>3f6f1cb0-3b00-45b5-91fd-d8553737eec7</ObjectId>
  <EncryptionType>3</EncryptionType>
</Credential>
```

Response Code: 200

### JSON Example

```
GET https://<Connection-server>/vmrest/users/<user-objectid>/credential/password
Accept: application/json
Content-type: application/json
Connection: keep-alive
```

The following is the response from the above \*GET\* request and the actual response will depend upon the information given by you:

```
{
  ?URI?: ?/vmrest/users/9375d893-c8eb-437b-90bf-7de4b1d0c3e8/credential/password?
  ?UserObjectId?: ?9375d893-c8eb-437b-90bf-7de4b1d0c3e8?
  ?CredentialType?: ?3?
  ?Credentials?
  ?IsPrimary?: ?false?
  ?CantChange?: ?false?
  ?DoesntExpire?: ?true?
  ?TimeChanged?: ?2013-03-05 11:24:33.344?
  ?HackCount?: ?5?
  ?Locked?: ?true?
  ?TimeLastHack?: ?2013-03-11 10:23:30.581?
  ?TimeLockout?: ?2013-03-05 11:24:33.344?
  ?Alias?: ?Texoma?
  ?CredMustChange?: ?true?
  ?CredentialPolicyObjectId?: ?a97ff291-8e60-475a-b7ee-e956ae83a730?
```

## Cisco\_Unity\_Connection\_Provisioning\_Interface\_(CUPI)\_API\_--\_User\_Password\_PIN\_Settings

```
?Hacked?: ?false?  
?ObjectId?: ?3f6f1cb0-3b00-45b5-91fd-d8553737eec7?  
?EncryptionType?: ?3?  
}
```

Response Code: 200

### Update Password/PIN Settings

For PIN:

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/pin
```

For Password:

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/password
```

```
<Credential>  
  <Locked>>false</Locked>  
  <DoesntExpire>>true</DoesntExpire>  
  <CredMustChange>>true</CredMustChange>  
  <CredentialPolicyObjectId>43e16996-57c6-46c4-86c0-f37d2edf0385</CredentialPolicyObjectId>  
</Credential>
```

The following is the response from the above \*PUT\* request and the actual response will depend upon the information given by you:

Response Code: 204

### Unlock Password/PIN Settings

A user's PIN is the password that a user must enter over the phone to sign into their mailbox to listen or send new messages by phone. To change a user's PIN you need the object ID of the user. A user's password is the web application password that is required to interact with web applications, such as the Cisco PCA or the Inbox applications.

For Password:

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/password
```

For PIN:

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/pin
```

```
<Credential>  
  <HackCount>0</HackCount>  
  <TimeHacked></TimeHacked>  
</Credential>
```

The following is the response from the above \*PUT\* request and the actual response will depend upon the information given by you:

Response Code: 204

### JSON Example:

## To Unlock Password

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/password
Accept: application/json
Content-type: application/json
Connection: keep-alive
Response Body:
{
  "HackCount": "0",
  "TimeHacked": ""
}
```

The following is the response from the above \*PUT\* request and the actual response will depend upon the information given by you:

Response Code: 204

## Change Password/PIN

For Password: PUT

```
https://<Connection-server>/vmrest/users/<user-objectid>/credential/password
```

For PIN:

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/pin
```

```
<Credential>
  <Credentials>ciscfo1234</Credentials>
</Credential>
```

The following is the response from the above \*PUT\* request and the actual response will depend upon the information given by you:

Response Code: 204

## JSON Example:

To Update PIN

```
PUT https://<Connection-server>/vmrest/users/<user-objectid>/credential/pin
Accept: application/json
Content-type: application/json
Connection: keep-alive
Response Body:
{
  "Credentials": "cisco1234"
}
```

The following is the response from the above \*PUT\* request and the actual response will depend upon the information given by you:

Response Code: 204

**Explanation of Data Fields**

| Field Name               | Data Type   | Operation  | Description  |
|--------------------------|-------------|------------|--|
| Locked                   | Boolean     | Read/Write | <p>A flag indicating whether access to the user account associated with this set of credentials is locked.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> <p>Default value: false</p>   |
| CantChange               | Boolean     | Read/Write | <p>A flag indicating whether the user can set this credential.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• false: User can change credential</li> <li>• true: User cannot change credential</li> </ul> <p>Default Value: false</p>  |
| CredMustChange           | Boolean     | Read/Write | <p>A flag indicating whether the user must change their credentials (PIN or password) at the next login.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> <p>Default Value :true</p>  |
| DoesntExpire             | Boolean     | Read/Write | <p>A flag indicating whether this user credential will expire, and therefore the user must change the credential periodically. However, if the credential does not expire (value = "true"), the user still may change the credential (if allowed by CantChange).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> <p>Default value: false</p> |
| CredentialPolicyObjectId | String(36)  | Read/Write | <p>The unique identifier of the CredentialPolicy object that is associated with this credential. Value for this parameter can be fetched from the objectId parameter. Response of the following URI:<br/>GET:<a href="https://&lt;connection-server&gt;/vmrest/credentialpolicies">https://&lt;connection-server&gt;/vmrest/credentialpolicies</a>.</p>  |
| TimeChanged              | datetime(8) | Read/Write | <p>The date and time when the credentials were last changed. The date and time is recorded in this column whenever a</p>   |

Cisco\_Unity\_Connection\_Provisioning\_Interface\_(CUPI)\_API\_--\_User\_Password\_PIN\_Settings

|                |                |            |   |
|----------------|----------------|------------|---|
|                |                |            | user credential is created or changed.  |
| HackCount      | Integer(4)     | Read/Write | The number of logon attempted that failed due to invalid credentials. The Unity system or external authentication provider determined that the credentials supplied as part of a user logon attempt were invalid.<br><br>Default value: 0   |
| TimeLastHack   | datetime(8)    | Read/Write | The date and time of the last logon attempt with an invalid user credential.  |
| TimeLockout    | datetime(8)    | Read/Write | The date and time that the credential was locked by an administrator.   |
| TimeHacked     | datetime(8)    | Read/Write | The date and time that the credential was locked due to too many hacks. The date and time is recorded in this column whenever a user credential is locked due to too many hacks based on the credential policy.   |
| ObjectId       | String (36)    | Read Only  | Unique identifier for the password/pin  |
| Credentials    | String(256)    | Read/Write | The PIN or password, for a user. The credentials are stored in an encrypted format.   |
| Alias          | String(64)     | Read/Write | A unique text name of the user.   |
| Hacked         | Boolean        | Read/Write | A flag indicating whether access to the user account associated with this set of credentials is locked due too many hack attempts.<br><br>Possible Values:<br><ul style="list-style-type: none"><li>• true</li><li>• false</li></ul><br>Default Value: false                                |
| EncryptionType | Integer        | Read/Write | Type of encryption that was used to generate the credentials.<br><br>Possible values:(0-5)<br><ul style="list-style-type: none"><li>• UNKNOWN: 0</li><li>• HASH_MD5: 1</li><li>• HASH_SHA1: 2</li><li>• HASH_IMS: 3</li><li>• REVERSIBLE: 4</li><li>• NONE: 5</li></ul><br>Default Value: 0 |
| CredentialType | CredentialType | Read/Write | The type of credential such as password, PIN, Windows or Domino credential.<br><br><ul style="list-style-type: none"><li>• 4- for PIN</li></ul>   |

Cisco\_Unity\_Connection\_Provisioning\_Interface\_(CUPI)\_API\_--\_User\_Password\_PIN\_Settings

|  |  |  |                   |
|--|--|--|-------------------|
|  |  |  | • 3- for Password |
|--|--|--|-------------------|