Configure Provisioning Profiles

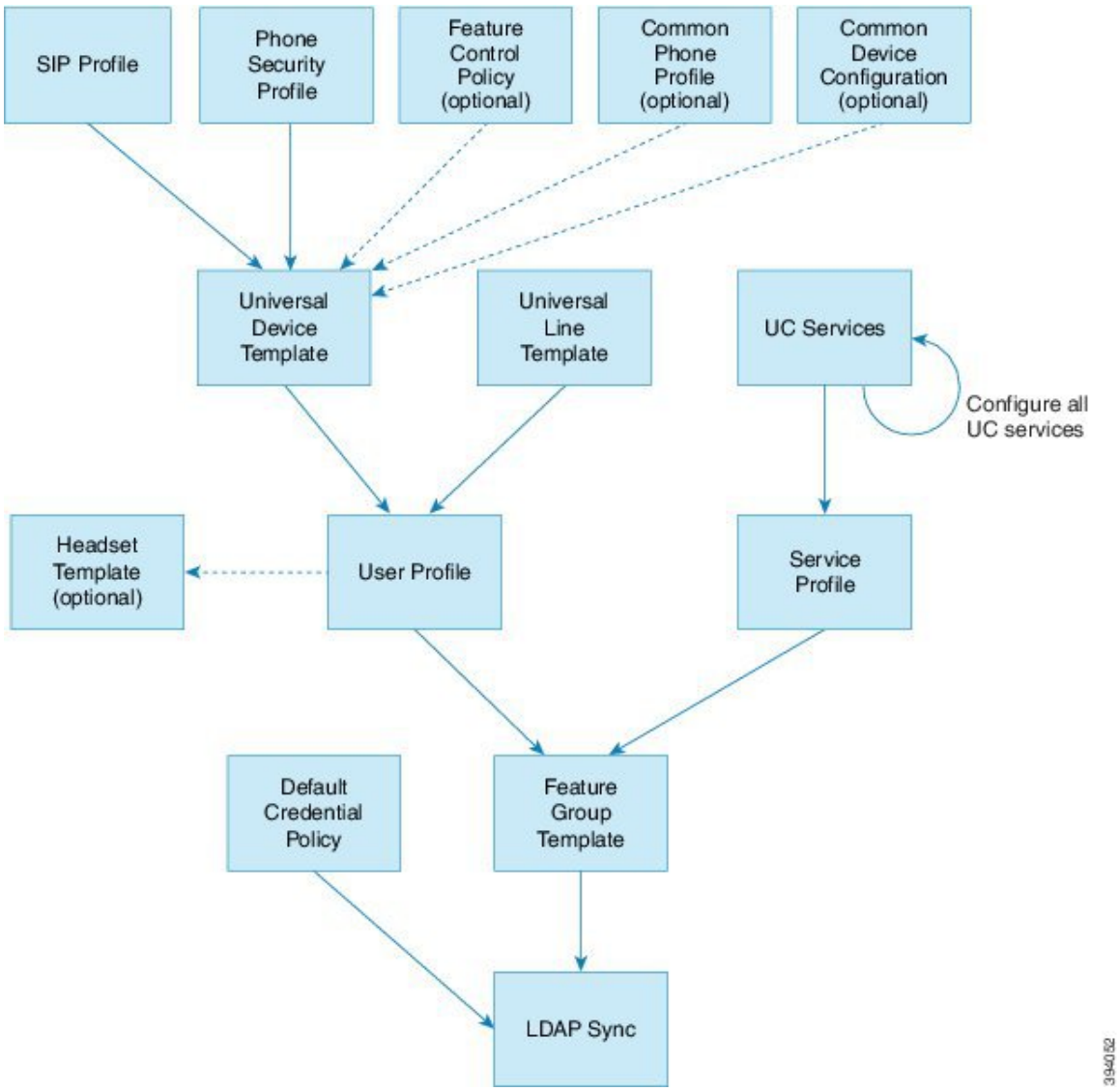
- Provisioning Profiles Overview, on page 1
- Provisioning Profiles Task Flow, on page 2
- Configure SIP Profile, on page 4
- Configure Phone Security Profile, on page 5
- Create a Feature Control Policy, on page 5
- Create a Common Phone Profile, on page 6
- Configure Common Device Configuration, on page 7
- Configure a Universal Device Template, on page 7
- Configure a Universal Line Template, on page 8
- Configure a User Profile, on page 9
- Configure a Headset Template, on page 10
- Configure UC Services, on page 11
- Configure a Service Profile, on page 12
- Configure a Feature Group Template, on page 12
- Configure Default Credential Policy, on page 13

Provisioning Profiles Overview

Unified Communications Manager contains a set of profiles and templates that you can assign to new users. If you set these profiles and common settings beforehand, when you provision new users, and assign devices, users and devices will be configured automatically based on the settings that are applied.

When you provision users, associate them to the User Profile and Service Profile that contain the settings they need. In addition, when you add devices for users, their device and directory number will be configured quickly using the Universal Line and Universal Device Templates that are associated to the user's User Profile.

You can use the following profiles and templates to apply common settings to users and endpoints based on the user needs.



Provisioning Profiles Task Flow

If you have a large number of users and devices to provision, you can simplify the configuration process by setting up user profiles and service profiles with templates and common settings that apply for users in a specific group (for example, customer support).

When you provision users, associate them to the User Profile and Service Profile that contain the settings they need. In addition, when you add devices for users, their device and directory number will be configured quickly using the Universal Line and Universal Device Templates that are associated to the user's User Profile.

You can use the following profiles and templates to apply common settings to users and endpoints based on the user needs.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profile, on page 4	Set up common SIP settings that will be associated with the SIP endpoints that you deploy.
Step 2	Configure Phone Security Profile, on page 5	Configure security profiles that you will assign to provisioned endpoints. Assign settings such as TLS and TFTP encryption.
Step 3	Create a Feature Control Policy, on page 5	**Optional**. Use this policy to enable particular features and control the appearance of phone softkeys.
Step 4	Create a Common Phone Profile, on page 6	**Optional**. Use this profile to assign TFTP data and product-specific configuration defaults to a profile that you can assign to groups of endpoints.
Step 5	Configure Common Device Configuration, on page 7	**Optional**. Use this configuration to assign user-specific settings and IPv6 preferences to endpoints.
Step 6	Configure a Universal Device Template, on page 7	This template contains common settings that will be used to configure newly provisioned phones. You can also assign the profiles that you've configured to this template.
Step 7	Configure a Universal Line Template, on page 8	This template contains common settings that will used to configure newly provisioned extensions. You can also configure enterprise and E.164 numbers for your extensions.
Step 8	Configure a User Profile, on page 9	Set up a User Profile with the device templates, line templates, and common settings for newly provisioned users.
Step 9	Configure a Headset Template, on page 10	**Optional**. If you plan to use Cisco Headsets configure headset templates and assign them to the User Profiles that you've set up.
Step 10	Configure UC Services, on page 11	Configure UC Services such as the IM and Presence Service and a directory service.
Step 11	Configure a Service Profile, on page 12	Create a Service Profile that includes the UC services you want to assign to provisioned users.
Step 12	Configure a Feature Group Template, on page 12	For LDAP syncs, add your user profile and service profiles to a feature group template that you can assign to LDAP-synced users.

	Command or Action	Purpose
Step 13	Configure Default Credential Policy, on page 13	Configure the credential policy that you will assign to newly provisioned users.

What to do next

- Set up your LDAP sync in order to provision new users
- If you are not deploying LDAP, you can use Bulk Administration to provision users by bulk.

Configure SIP Profile

Use this procedure to configure a SIP profile with common SIP settings that you can assign to SIP devices.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Device Settings > SIP Profile**.

Step 2 Perform one of the following steps:

- To edit an existing profile, click **Find** and select the SIP profile.
- To create a new profile, click **Add New**.

Step 3 Enter a **Name** for the profile.

Step 4 If you are deploying URI dialing, configure the **Dial String Interpretation** to instruct the system on whether to handle calls as directory URIs or phone numbers.

Step 5 Under **Parameters Used in Phone**, complete the DSCP settings to define QoS handling for types of calls that use this profile.

Step 6 (Optional) If you need to assign a Normalization Script, select one of the default scripts from the Normalization Script drop-down list.

Note
You can also create your own scripts. For details, see the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Step 7 If you want this profile to support both IPv4 and IPv6 stacks simultaneously, check the **Enable ANAT** check box.

Step 8 Check the **Allow Presentation Sharing using BFCP** check box if you want your users to be able to share presentations.

Step 9 Complete the remaining fields in the SIP Profile Configuration window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

Configure Phone Security Profile

If you want to enable security features like TLS signaling, CAPF, and digest authentication requirements for the endpoints, you must configure a new security profile that you can apply it to the endpoints.

Note By default, if you don't apply a SIP phone security profile to a provisioned device, the device uses a nonsecure profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Click **Add New**.

Step 3 From the **Phone Security Profile Type** drop-down list, choose the Universal Device Template to create a profile that you can use when provisioning through the device templates.

Note
Optionally, you can also create security profiles for specific device models.

Step 4 Select the protocol.

Step 5 Enter an appropriate name for the profile in the **Name** field.

Step 6 If you want to use TLS signaling to connect to the device, set the **Device Security Mode** to **Authenticated** or **Encrypted** and the Transport Type to **TLS**.

Step 7 (Optional) Check the **Enable OAuth Authentication** check box if you want the phone to use digest authentication.

Step 8 (Optional) Check the **TFTP Encrypted Config** check box if you want to use encrypted TFTP.

Step 9 Complete the remaining fields in the Phone Security Profile Configuration window. For help with the fields and their settings, see the online help.

Step 10 Click **Save**.

Create a Feature Control Policy

Follow these steps to create a feature control policy. Use this policy to enable or disable a particular feature and hence control the appearance of softkeys that display on the phone.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Feature Control Policy**.

Step 2 Perform one of the following tasks:

- To modify the settings for an existing policy, enter search criteria, click **Find** and choose the policy from the resulting list.
- To add a new policy, click **Add New**.

The **Feature Control Policy Configuration** window is displayed.

Step 3 In the **Name** field, enter a name for the feature control policy.

Step 4 In the **Description** field, enter a brief description for the feature control policy.

Step 5 In the **Feature Control Section**, for each feature listed, choose whether you want to override the system default and enable or disable the setting:

- If the feature is enabled by default and you want to disable the setting, check the check box under **Override Default** and uncheck the check box under **Enable Setting**.
- If the feature is disabled by default and you want to enable the setting, check the check box under **Override Default** and check the check box under **Enable Setting**.

Step 6 Click **Save**.

Create a Common Phone Profile

A common phone profile is an optional profile that can be used to configure TFTP data and Product-Specific Configuration defaults for the phones that use the profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Device Settings > Common Phone Profile** menu path to configure common phone profiles.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the profile.

Step 4 Enter a **Description** for the profile.

Step 5 If you set up a **Feature Control Policy** to phones that use this profile, select the policy from the drop-down list.

Step 6 Complete the remaining fields in the **Common Phone Profile Configuration** window. For help with the fields and their settings, see the online help.

Step 7 Configure fields under Product-Specific Configuration Layout. For field descriptions, click the (?) to see field-specific help.

Step 8 (Optional) If you want to enable Interactive Connectivity Establishment (ICE) for Mobile and Remote Access phones:

a) Set the ICE drop-down to **Enabled**.

b) Set the **Default Candidate Type** to one of the following:

- **Host**—A candidate obtained by selecting the IP address on the host device. This is the default.
- **Server Reflexive**—An IP address and port candidate obtained by sending a STUN request. Often, this may represent the public IP address of the NAT.

- **Relayed**—An IP address and port candidate obtained from a TURN server. The IP address and port are resident on the TURN server such that media is relayed through the TURN server.

c) Configure the remaining ICE fields.

Step 9 Click **Save**.

Configure Common Device Configuration

A common device configuration comprises a set of optional set of user-specific feature attributes. If you are deploying IPv6, you can use this configuration to assign IPv6 preferences for SIP trunks or SCCP phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Click **Add New**.

Step 3 For SIP trunks, SIP Phones or SCCP phones, choose a value for the **IP Addressing Mode** drop-down list:

- **IPv4 Only**—The device uses only an IPv4 address for media and signaling.
- **IPv6 Only**—The device uses only an IPv6 address for media and signaling.
- **IPv4 and IPv6 (Default)**—The device is a dual-stack device and uses whichever IP address type is available. If both IP address types are configured on the device, for signaling the device uses the **IP Addressing Mode Preference for Signaling** setting and for media the device uses the **IP Addressing Mode Preference for Media** enterprise parameter setting.

Step 4 If you configure IPv6 in your previous step, then configure an IP addressing preference for the **IP Addressing Mode for Signaling** drop-down list:

- **IPv4**—The dual stack device prefers IPv4 address for signaling.
- **IPv6**—The dual stack device prefers IPv6 address for signaling.
- **Use System Default**—The device uses the setting for the **IP Addressing Mode Preference for Signaling** enterprise parameter.

Step 5 Configure the remaining fields in the **Common Device Configuration** window. For more information on the fields and their configuration options, see the system Online Help.

Step 6 Click **Save**.

Configure a Universal Device Template

Universal device templates make it easy to apply configuration settings to newly provisioned devices. The provisioned device uses the settings of the universal device template. You can configure different device templates to meet the needs of different groups of users. You can also assign the profiles that you've configured to this template.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Click **Add New**.

Step 3 Enter the following mandatory fields:

a) Enter a **Device Description** for the template.
b) Select a **Device Pool** type from the drop-down list.
c) Select a **Device Security Profile** from the drop-down list.
d) Select a **SIP Profile** from the drop-down list.
e) Select a **Phone Button Template** from the drop-down list.

Step 4 Complete the remaining fields in the **Universal Device Template Configuration** window. For field descriptions, see the online help.

Step 5 Under **Phone Settings**, complete the following optional fields:

a) If you configured a **Common Phone Profile**, assign the profile.
b) If you configured a **Common Device Configuration**, assign the configuration.
c) If you configured a **Feature Control Policy**, assign the policy.

Step 6 Click **Save**.

Configure a Universal Line Template

Universal Line Templates make it easy to apply common settings to newly assigned directory numbers. Configure different templates to meet the needs of different groups of users.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Line Template**.

Step 2 Click **Add New**.

Step 3 Configure the fields in the **Universal Line Template Configuration** window. See the online help for more information about the fields and their configuration options.

Step 4 If you are deploying Global Dial Plan Replication with alternate numbers expand the **Enterprise Alternate Number** and **+E.164 Alternate Number** sections and do the following:

a) Click the **Add Enterprise Alternate Number** button and/or **Add +E.164 Alternate Number** button.
b) Add the **Number Mask** that you want to use to assign to your alternate numbers. For example, a 4-digit extension might use 5XXXX as an enterprise number mask and 1972555XXXX as an +E.164 alternate number mask.
c) Assign the partition where you want to assign alternate numbers.

d) If you want to advertise this number via ILS, check the **Advertise Globally via ILS** check box. Note that if you are using advertised patterns to summarize a range of alternate numbers, you may not need to advertise individual alternate numbers.
e) Expand the **PSTN Failover** section and choose the **Enterprise Number** or **+E.164 Alternate Number** as the PSTN failover to use if normal call routing fails.

Step 5 Click **Save**.

Configure a User Profile

Assign universal line and universal device template to users through the User Profile. Configure multiple user profiles for different groups of users. You can also enable self-provisioning for users who use this service profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **User Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the user profile.

Step 4 Assign a **Universal Device Template** to apply to users' **Desk Phones**, **Mobile and Desktop Devices**, and **Remote Destination/Device Profiles**.

Step 5 Assign a **Universal Line Template** to apply to the phone lines for users in this user profile.

Step 6 If you want the users in this user profile to be able to use the self-provisioning feature to provision their own phones, do the following:

a) Check the **Allow End User to Provision their own phones** check box.
b) In the **Limit Provisioning once End User has this many phones** field, enter a maximum number of phones the user is allowed to provision. The maximum is 20.
c) Check the **Allow Provisioning of a phone already assigned to a different End User** check box to determine whether the user who is associated with this profile has the permission to migrate or reassign a device that is already owned by another user. By default, this check box is unchecked.

Step 7 If you want Cisco Jabber users who are associated with this user profile, to be able to use the Mobile and Remote Access feature, check the **Enable Mobile and Remote Access** check box.

Note

- By default, this check box is selected. When you uncheck this check box, the **Client Policies** section is disabled, and No Service client policy option is selected by default.
- This setting is mandatory only for Cisco Jabber users whom are using OAuth Refresh Logins. Non-Jabber users do not need this setting to be able to use Mobile and Remote Access. Mobile and Remote Access feature is applicable only for the Jabber Mobile and Remote Access users and not to any other endpoints or clients.

Step 8 Assign the Jabber policies for this user profile. From the **Desktop Client Policy**, and **Mobile Client Policy** drop-down list, choose one of the following options:

- No Service—This policy disables access to all Cisco Jabber services.
- IM & Presence only—This policy enables only instant messaging and presence capabilities.
- IM & Presence, Voice and Video calls—This policy enables instant messaging, presence, voicemail, and conferencing capabilities for all users with audio or video devices. This is the default option.

Note
Jabber desktop client includes Cisco Jabber for Windows users and Cisco Jabber for Mac users. Jabber mobile client includes Cisco Jabber for iPad and iPhone users and Cisco Jabber for Android users.

Step 9 If you want the users in this user profile to set the maximum login time for Extension Mobility or Extension Mobility Cross Cluster through Cisco Unified Communications Self Care Portal, check the **Allow End User to set their Extension Mobility maximum login time** check box.

Note
By default **Allow End User to set their Extension Mobility maximum login time** check box is unchecked.

Step 10 Click **Save**.

Configure a Headset Template

Use this procedure to configure a headset template with customized settings that you can apply to Cisco headsets. You can create a customized template or use the system-defined Standard Default Headset Template.

Note The Standard Default Headset Configuration Template is a system-defined template. You can assign new User Profiles to the Standard Default Headset Template but you can't edit the template. By default, all user profiles are assigned to this template. To disassociate a user profile from this template, you must assign the profile to a new template.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Headset > Headset Template**.

Step 2 Do either of the following:

- To edit an existing template, select the template.
- To create a new template, select any existing template and click **Copy**. The existing settings are applied to your new template.

Step 3 Add a **Name** and **Description** for the template.

Step 4 Under **Model and Firmware Settings**, assign any customized headset settings that you want to apply to this template. To add a new setting, click the **Add** button and configure the settings.

Step 5 Use the up and down arrows to move the User Profiles that you want to assign to this template to the **Assigned Users Profiles** list box. All users whom are assigned to those profiles will also be assigned to this headset template.

Step 6 Click **Save**.

Step 7 Use the **Set to Default** button to return to the default template settings.

Step 8 Click **Apply Config**.

For a Standard Default Headset Configuration Template, the **Apply Config** button takes effect for the following:

- Devices owned by users you added to the Assigned User Profile list
- Anonymous devices

For a Customized Headset Configuration Template, the **Apply Config** button takes effect only for devices owned by users you added to the **Assigned User Profiles** list.

Configure UC Services

Use this procedure to configure the UC service connections that your users will use. You can configure connections for the following UC services:

- Voicemail
- Mailstore
- Conferencing
- Directory
- IM and Presence Service
- CTI
- Video Conferencing Scheduling Portal
- Jabber Client Configuration (jabber-config.xml)

Note The fields may vary depending on which UC service you configure.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management > User Settings > UC Services**.

Step 2 Click **Add New**.

Step 3 From the UC Service Type drop-down, select the UC service that you want to configure and click **Next**.

Step 4 Select the **Product Type**.

Step 5 Enter a **Name** for the service.

Step 6 Enter the **Hostname or IP address** for the server where the service is homed.

Step 7 Complete the **Port** and **Protocol** information.

Step 8 Configure the remaining fields. For help with the fields and their settings, refer to the online help. The field options vary depending on which UC service you are deploying.

Step 9 Click **Save**.

Step 10 Repeat this procedure until you have provisioned all the UC services that you need.

Note
If you want the service to be located on multiple servers, configure different UC service connections that point to different servers. For example, with the IM and Presence Service Centralized Deployment, it is recommended to configure multiple IM and Presence UC services that point to different IM and Presence nodes. After you have configured all your UC connections, you can add them to a Service Profile.

Configure a Service Profile

Configure a Service Profile that include the UC Services that you want to assign to end users who use the profile.

Before you begin

You must set up your Unified Communications (UC) services before you can add them to a service profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Service Profile**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** for the chosen Service Profile Configuration.

Step 4 Enter a **Description** for the chosen Service Profile Configuration.

Step 5 For each UC service that you want to be a part of this profile, assign the **Primary**, **Secondary**, and **Tertiary** connections for that service.

Step 6 Complete the remaining fields in the **Service Profile Configuration** window. For detailed field descriptions, see the online help.

Step 7 Click **Save**.

Configure a Feature Group Template

Feature group templates aid in your system deployment by helping you to quickly configure phones, lines, and features for your provisioned users. If you are syncing users from a company LDAP directory, configure a feature group template with the User Profile and Service Profile that you want users synced from the directory to use. You can also enable the IM and Presence Service for synced users through this template.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Feature Group Template**.

Step 2 Click **Add New**.

Step 3 Enter a **Name** and **Description** for the Feature Group Template.

Step 4 Check the **Home Cluster** check box if you want to use the local cluster as the home cluster for all users whom use this template.

Step 5 Check the **Enable User for Unified CM IM and Presence** check box to allow users whom use this template to exchange instant messaging and presence information.

Step 6 From the drop-down list, select a **Services Profile** and **User Profile**.

Step 7 Complete the remaining fields in the **Feature Group Template Configuration** window. Refer to the online help for field descriptions.

Step 8 Click **Save**.

What to do next

Associate the feature group template with an LDAP directory sync to apply the settings from the template to synchronized end users.

Configure Default Credential Policy

Use this procedure to configure clusterwide default credential policies that get applied to newly provisioned users. You can apply a separate credential policy for each of the following credential types:

- Application User Passwords
- End User Passwords
- End User PINs

Procedure

Step 1 Configure settings for a credential policy:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.

b) Do either of the following:

- Click **Find** and select an existing credential policy.
- Click **Add New** to create a new credential policy.

c) If you want the system to check for easily hacked passwords such as ABCD or 123456, check the **Check for Trivial Passwords** check box.

d) Complete the fields in the **Credential Policy Configuration** window. For help with the fields and their settings, see the online help.
e) Click **Save**.
f) If you want to create a different credential policy for one of the other credential types, repeat these steps.

Step 2 Apply the credential policy to one of the credential types:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.
b) Select the credential type to which you want to apply your credential policy.
c) From the **Credential Policy** drop-down, select the credential policy that you want to apply for this credential type. For example, you might select the credential policy that you created.
d) Enter the default passwords in both the **Change Credential** and **Confirm Credential** fields. Users have to enter these passwords at next login.
e) Configure the remaining fields in the **Credential Policy Default Configuration** window. For help with the fields and their settings, see the online help.
f) Click **Save**.
g) If you want to assign a credential policy for one of the other credential types, repeat these steps.

Note For individual users, you can also assign a policy to a specific user credential from the **End User Configuration** window or **Application User Configuration** window for that user. Click the **Edit Credential** button that is adjacent to the credential type (password or PIN) to open the **Credential Configuration** settings for that user credential.