CHAPTER 15

DCNM-LAN 認証設定の管理

この章では、Cisco Data Center Network Manager for LAN（DCNM-LAN）の認証設定を管理する方法について説明します。

この章の内容は、次のとおりです。

DCNM-LAN 認証設定の管理の概要

DCNM-LAN 認証設定は、DCNM-LAN クライアントを使用してサーバにアクセスを試みるユーザを DCNM-LAN サーバが認証する方法を決定します。また、ユーザのユーザ ロールを決定します。これは、DCNM-LAN クライアントでユーザが設定できる内容に影響を与えます。

ここでは、次の内容について説明します。

ユーザとユーザ ロール

DCNM-LAN には、DCNM-LAN クライアントを使用して DCNM-LAN サーバにアクセスできるユーザを制御できるユーザベースのアクセスが実装されています。ユーザ アクセスはパスワードで保護されます。DCNM-LAN は強力なパスワードをサポートしています。

DCNM-LAN にアクセスするそれぞれの人が一意のユーザ アカウントを持つようにすることで、ユーザベースのアクセスにより、各ユーザが実行できる操作を決定できます。

また、DCNM-LAN では、各ユーザにロールを割り当てることができます。ロールは、DCNM-LAN クライアントでユーザが実行できる操作を決定します。表 15-1 に示すとおり、DCNM-LAN では 2 つのユーザ ロールがサポートされています。

表 15-1　DCNM-LAN のユーザ ロール

DCNM-LAN ロール	説明
User	• DCNM-LAN 認証モードを変更できません • DCNM-LAN ローカル ユーザ アカウントを追加または削除できません • 自身のローカル ユーザ アカウントの詳細を変更できます • その他の機能もすべて使用できます
Administrator	• DCNM-LAN 認証設定を完全に制御できます • その他の機能もすべて使用できます

ローカル認証と DCNM-LAN ローカル ユーザ

DCNM-LAN データベースには、作成するすべての DCNM-LAN ローカル ユーザが格納されます。

（注） DCNM-LAN サーバのユーザは、DCNM-LAN サーバにローカルです。DCNM-LAN サーバ ユーザを作成、変更、削除しても、管理対象デバイス上のユーザ アカウントには影響がありません。

DCNM-LAN サーバは、次の場合にローカル ユーザを使用してアクセスを許可します。

- 認証モードがローカルである場合
- 現在の認証モードの認証サーバに到達できない場合。

ローカル認証を第一の認証モードとして使用できます。RADIUS または TACACS+ を第一の認証モードとして指定し、現在の認証モードの認証サーバに到達できない場合、DCNM-LAN サーバはローカル認証にフォールバックします。

RADIUS および TACACS+ 認証

DCNM-LAN を、RADIUS または TACACS+ AAA プロトコルを使用してユーザを認証するように設定できます。

DCNM-LAN では、RADIUS と TACACS+ に対して、プライマリ、セカンダリ、およびターシャリ認証サーバがサポートされています。必須なのはプライマリ サーバだけです。各認証サーバに対し、サーバが認証要求を待ち受けるポート番号を指定できます。

認証の際、現在の認証モードのプライマリ サーバが認証要求に応答しない場合、DCNM-LAN サーバは認証要求をセカンダリ サーバに送信します。セカンダリ サーバが応答しない場合、DCNM-LAN は認証要求をターシャリ サーバに送信します。

現在の認証モードに対して設定されているサーバのどれも認証要求に応答しない場合、DCNM-LAN サーバはローカル認証にフォールバックします。

RADIUS および TACACS+ によるユーザ ロールの割り当て

DCNM-LAN は、RADIUS または TACACS+ サーバによるユーザ ロールの割り当てをサポートしています。ユーザ ロールは、DCNM-LAN クライアントにユーザ アクセスを許可します。ユーザに割り当てられるユーザ ロールは、DCNM-LAN クライアントの現在のセッションだけに影響を与えます。

DCNM-LAN ユーザ ロールを RADIUS によって割り当てるには、RADIUS のベンダー固有属性 26/9/1（Cisco-AV-Pair 属性）を返すように RADIUS サーバを設定します。DCNM-LAN ユーザ ロールを TACACS+ によって割り当てるには、TACACS+ サーバから cisco-av-pair の属性と値のペアが返される必要があります。認証応答でユーザ ロールが割り当てられない場合、DCNM-LAN によってユーザ ロールが割り当てられます。表 15-2 に、各 DCNM-LAN ユーザ ロールに対してサポートされる属性と値のペアの値を示します。

表 15-2　DCNM-LAN ユーザ ロールの割り当て値

DCNM-LAN ロール	RADIUS Cisco-AV-Pair の値	TACACS+ Shell Cisco 属性と値（AV）のペアの値
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

ローカル認証へのフォールバック

ローカル認証は、常に RADIUS および TACACS+ 認証モードのフォールバック手段になります。現在の認証モードに対して設定されているサーバのどれも使用できない場合、DCNM-LAN サーバは、ローカル データベースを使用してログイン要求を認証します。この動作により、DCNM-LAN からの意図しないロックアウトを回避できます。

フォールバック サポートが必要なユーザに対して、そのローカル ユーザ アカウントのユーザ名は、認証サーバのユーザ名と同じである必要があります。また、透過的なフォールバックのサポートを実現するために、ローカル ユーザ アカウントのパスワードも認証サーバ上のパスワードと同じにすることをお勧めします。ユーザは、認証サーバとローカル データベースのどちらで認証サービスが提供されているかを判断できないため、認証サーバとローカル データベースで異なるユーザ名とパスワードを使用すると、ユーザはどのユーザ名とパスワードを指定すべきかわからなくなります。

パスワード回復

DCNM-LAN クライアントに誰も DCNM-LAN Administrator ロールを持つユーザとしてログインできない場合、次のいずれかのスクリプトを使用してパスワードをリセットできます。

- Microsoft Windows の場合は、*dcnm_root_directory*/dcm/dcnm/bin/pwreset.bat を使用します（デフォルトでは、*dcnm_root_directory* は c:¥Program Files¥Cisco Systems¥dcm¥dcnm¥bin です）。
- Linux の場合は、*dcnm_root_directory*/dcm/dcnm/bin/pwreset.sh を使用します（デフォルトでは、*dcnm_root_directory* は /usr/local/cisco です）。

パスワードをリセットするには、使用しているオペレーティング システム用のスクリプトを実行し、リセットするユーザ ID とそのユーザ ID で使用するパスワードを入力します。

または、DCNM-LAN サーバを再インストールすることで、Administrator ロールに割り当てるローカル ユーザ アカウントのユーザ名とパスワードを指定できます。詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

ユーザとデバイス クレデンシャル

ユーザがローカル ユーザ アカウントを使用して認証されるか、RADIUS または TACACS+ サーバ上のアカウントを使用して認証されるかにかかわらず、DCNM-LAN サーバの各ユーザには一意のデバイス クレデンシャルがあります。この機能により、DCNM-LAN サーバの各ユーザの操作が反映されたアカウンティング ログを管理対象デバイス上に保持できます。詳細については、「デバイスとクレデンシャルの概要」（P.17-1）を参照してください。

仮想化のサポート

Cisco NX-OS による仮想デバイス コンテキストのサポートは、DCNM-LAN サーバ ユーザに影響を及ぼしません。

DCNM-LAN サーバ ユーザは任意の管理対象デバイスを設定できます。

DCNM-LAN 認証設定を管理するためのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco DCNM-LAN	Cisco DCNM-LAN 認証設定を管理するためにライセンスは必要ありません。ライセンス パッケージに含まれていない機能は Cisco DCNM-LAN にバンドルされており、無料で提供されます。Cisco DCNM-LAN LAN エンタープライズ ライセンスの取得とインストールの詳細については、『*Cisco DCNM Installation and Licensing Guide, Release 5.x*』を参照してください。

DCNM-LAN 認証設定を管理するための前提条件

DCNM-LAN 認証設定の管理には次の前提条件があります。

- DCNM-LAN とともに使用するすべての認証サーバが、DCNM-LAN サーバからの認証要求を受け付けるように設定する必要があります。DCNM-LAN をクラスタ サーバ環境に展開している場合には、すべての認証サーバが、クラスタ内の各 DCNM-LAN サーバからの要求を受け付けるように設定します。
- DCNM-LAN ローカル ユーザを追加、削除、変更するには、DCNM-LAN の Administrator ロールに割り当てられたユーザ アカウントを使用して DCNM-LAN クライアントにログインする必要があります。

DCNM-LAN 認証設定の管理に関する注意事項と制約事項

DCNM-LAN 認証設定の管理における注意事項と制約事項は次のとおりです。

- DCNM-LAN クライアントを使用するユーザごとに DCNM-LAN ユーザ アカウントを作成します。複数の人でユーザ アカウントを共有しないようにします。
- 使用していない DCNM-LAN ユーザ アカウントは削除します。
- 管理者ユーザ アカウントは、DCNM-LAN クライアントで管理タスクを行う必要があるユーザだけに与えます。
- 強力なパスワードの使用を推奨します。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

DCNM-LAN 認証の設定

ここでは、次の内容について説明します。

認証モードの設定

DCNM-LAN サーバが DCNM-LAN クライアント ユーザを認証するために使用するモードを設定できます。

はじめる前に

Administrator ユーザ ロールを持つユーザ アカウントを使用して DCNM-LAN クライアントにログインします。

RADIUS または TACACS+ 認証モードをイネーブルにする場合は、目的とする認証モードに対して認証サーバを 1 台以上設定する必要があります。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Mode] セクションを展開します。

ステップ 3　認証モードを選択します。

ステップ 4　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

ステップ 5　DCNM-LAN サーバを再起動します。詳細については、第 28 章「Cisco DCNM-LAN サーバの起動と停止」を参照してください。

DCNM-LAN ローカル ユーザの追加

DCNM-LAN ローカル ユーザ アカウントを追加できます。

（注）　DCNM-LAN ローカル ユーザ アカウントを追加しても、Cisco NX-OS デバイス上のユーザ アカウント設定は影響を受けません。

はじめる前に

Administrator ユーザ ロールを持つユーザ アカウントを使用して DCNM-LAN クライアントにログインします。

新規の DCNM-LAN ローカル ユーザ アカウントのユーザ名とパスワードを決定します。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [Cisco DCNM Local Users] セクションに表示されます。

ステップ 3　メニュー バーで、[Actions] > [Add User] の順に選択します。

ユーザ リストの一番下に新規の行が表示されます。デフォルトでは、新規の行のすべてのフィールドは空白になっています。

ステップ 4　新規行の [DCNM User Name] 列にユーザ名を入力します。ユーザ名は 1 ～ 198 文字の範囲で指定します。文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 5　（任意）[Full Name] 列で、エントリをダブルクリックして、名前を追加します。たとえば、DCNM-LAN ローカル ユーザ アカウントを使用するユーザの本名を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 6　[DCNM Role] 列で、エントリをダブルクリックして、ロールを選択します。デフォルトのロールは「ユーザ」です。

ステップ 7　[Password] 列で、エントリをダブルクリックして、下矢印ボタンをクリックします。

ステップ 8　[New Password] フィールドと [Confirm Password] フィールドに、パスワードを入力します。パスワードは 1 ～ 255 文字の範囲で指定します。文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 9　[OK] をクリックします。

ステップ 10　（任意）[Description] 列で、エントリをダブルクリックして、ユーザ アカウントの説明を追加します。たとえば、この DCNM-LAN サーバ ユーザ アカウントを使用するユーザの電子メールや電話番号など、連絡先の詳細を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 11　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN ローカル ユーザのパスワードの変更

DCNM-LAN ローカル ユーザのパスワードを変更できます。

はじめる前に

自分が DCNM-LAN クライアントにログインするときに使用するアカウント以外のローカル ユーザ アカウントのパスワードを変更する場合は、Administrator ロールが必要です。ユーザ アカウントがローカル ユーザ アカウントで、User ロールが割り当てられている場合、自身のアカウントのパスワードだけを変更できます。

新規のパスワードを決定してください。

（注）　強力なパスワードを使用することをお勧めします。強力なパスワードの一般的なガイドラインとしては、パスワードの長さを 8 文字以上にすることや、少なくとも 1 つの文字、数字、および記号を使用することなどが挙げられます。たとえば、Re1Ax@h0m3 というパスワードは 10 文字で、1 つの記号と 3 つの数字に加えて大文字と小文字が使用されています。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Server Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [DCNM Local Users] セクションに表示されます。

ステップ 3　[User Name] 列で、変更するユーザ アカウントのユーザ名をクリックします。

クリックしたユーザ名の行が強調表示されます。

ステップ 4　[Password] 列で、エントリをダブルクリックして、下矢印ボタンをクリックします。

ステップ 5　[New Password] フィールドと [Confirm Password] フィールドに、新規のパスワードを入力します。パスワードは 1 ～ 255 文字の範囲で指定します。文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 6　[OK] をクリックします。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN ローカル ユーザのフルネーム、ロール、説明の変更

DCNM-LAN ローカル ユーザのフルネーム、ロール、説明を変更できます。

（注）　ユーザ名は変更できません。代わりに、使用するユーザ名を持つローカル ユーザ アカウントを追加して、使用しないユーザ名を持つローカル ユーザ アカウントを削除します。

はじめる前に

新しいフルネームまたは説明を決定してください。

自分が DCNM-LAN クライアントにログインするときに使用するローカル ユーザ アカウント以外のローカル ユーザ アカウントのフルネーム、ロール、または説明を変更する場合は、Administrator ロールが必要です。ユーザ アカウントがローカル ユーザ アカウントで、User ロールが割り当てられている場合、自身のアカウントのフルネームと説明だけを変更できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [Cisco DCNM Local Users] セクションに表示されます。

ステップ 3　[User Name] 列で、変更するローカル ユーザ アカウントのユーザ名をクリックします。

クリックしたユーザ名の行が強調表示されます。

ステップ 4　（任意）[Full Name] 列で、エントリをダブルクリックして新しい名前を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 5　（任意）[DCNM Role] 列で、エントリをダブルクリックして、新規ロールを選択します。「管理者」または「ユーザ」を選択できます。

ステップ 6　（任意）[Description] 列で、エントリをダブルクリックして、ユーザ アカウントの説明を入力します。最大長は 255 文字で、文字（大文字と小文字を区別）、数字、記号を使用できます。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN サーバ ユーザの削除

DCNM-LAN ローカル ユーザ アカウントを削除できます。

はじめる前に

Administrator ユーザ ロールを持つユーザ アカウントを使用して DCNM-LAN クライアントにログインします。

削除しようとしている DCNM-LAN ローカル ユーザ アカウントが正しいことを確認してください。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [DCNM Local Users] セクションを展開します。

ユーザの表が [DCNM Local Users] セクションに表示されます。

ステップ 3　[User Name] 列で、削除するユーザ アカウントのユーザ名をクリックします。

クリックしたユーザ名の行が強調表示されます。

ステップ 4　メニュー バーで、[Actions] > [Delete User] の順に選択します。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

認証サーバの追加

RADIUS および TACACS+ サーバを DCNM-LAN 認証設定に追加できます。

はじめる前に

（注）　DCNM-LAN とともに使用するすべての認証サーバが、DCNM-LAN サーバからの認証要求を受け付けるように設定する必要があります。DCNM-LAN をクラスタ サーバ環境に展開している場合には、すべての認証サーバが、クラスタ内の各 DCNM-LAN サーバからの要求を受け付けるように設定します。

追加する各認証サーバについて次の情報を入手してあることを確認します。

- AAA プロトコル：RADIUS または TACACS+
- サーバの IPv4 アドレスまたは DCNM-LAN サーバが解決できる DNS 名。
- 秘密キー。
- サーバが認証要求を受け付けるポート番号。
- （RADIUS 限定）サーバがアカウンティング メッセージを受け付けるポート番号。
- 認証プロトコル：PAP、CHAP、MSCHAP、ASCII。
- （任意）サーバ確認用の、サーバ上の有効なユーザ アカウントのユーザ名とパスワード。

サーバをプライマリ、セカンダリ、ターシャリ サーバのどれにするかを決定します。これは、認証サーバのフェールオーバー戦略に依存します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　必要に応じて [RADIUS] または [TACACS+] サーバ行を展開します。

ステップ 4　追加する各認証サーバに対し、次の手順を実行します。

a. サーバを追加する行を選択します。

（注） プライマリ サーバを追加しないとセカンダリ サーバを追加できません。また、セカンダリ サーバを追加しないとターシャリ サーバを追加できません。

b. [Server Name] フィールドをダブルクリックし、サーバの IPv4 アドレスまたは DNS ホスト名を入力します。

（注） DCNM-LAN サーバが解決できないホスト名を入力すると、[Server Name] フィールドが赤く強調表示されます。

c. [Secret Key] フィールドをダブルクリックし、認証サーバの秘密キー（共有秘密キーとも呼びます）を入力します。

d. （任意）デフォルトの [Authentication Port] または [Accounting Port]（RADIUS 限定）を変更する必要がある場合は、該当するポート フィールドをダブルクリックし、新しいポート番号を入力します。

e. [Authentication Method] フィールドをダブルクリックし、DCNM-LAN から認証サーバに認証要求を送信するときに使用する認証プロトコルを選択します。

ステップ 5　（任意）DCNM-LAN サーバが新しい認証サーバを使用してユーザを認証できることを確認するには、次の手順を実行します。

a. 確認する認証サーバの行の右にある [Verify] をクリックします。

[Verification] ダイアログボックスが表示されます。

b. 認証サーバ上の有効なユーザ アカウントのユーザ名とパスワードを入力します。

c. [Verify] をクリックします。

DCNM-LAN クライアントに、確認が成功したか失敗したかを示すメッセージが表示されます。確認が失敗する場合、認証サーバが使用できないか、認証設定が正しくないことが考えられます。

ステップ 6　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

認証サーバ設定の変更

DCNM-LAN クライアントで設定済みの認証サーバの設定を変更できます。複数の RADIUS または TACACS+ サーバがある場合、どのサーバをプライマリ、セカンダリ、ターシャリにするかを変更できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　必要に応じて [RADIUS] または [TACACS+] サーバ行を展開します。

ステップ 4　（任意）認証サーバの設定を変更する場合は、変更する各フィールドをダブルクリックし、変更内容を入力します。

ステップ 5　（任意）RADIUS または TACACS+ サーバの順序を変更する場合は、サーバを右クリックし、[Move Up] または [Move Down] のいずれかを選択します。

ステップ 6　（任意）DCNM-LAN サーバが認証サーバを使用してユーザを認証できることを確認するには、次の手順を実行します。

a. 確認する認証サーバの行の右にある [Verify] をクリックします。

[Verification] ダイアログボックスが表示されます。

b. 認証サーバ上の有効なユーザ アカウントのユーザ名とパスワードを入力します。

c. [Verify] をクリックします。

DCNM-LAN クライアントに、確認が成功したか失敗したかを示すメッセージが表示されます。確認が失敗する場合、認証サーバが使用できないか、認証設定が正しくないことが考えられます。

ステップ 7　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

認証サーバの削除

RADIUS または TACACS+ の認証サーバを DCNM-LAN 認証設定から削除できます。

はじめる前に

現在の認証モードのすべての認証サーバの削除はできません。代わりに、まず認証モードを変更し、次にすべての認証サーバを削除します。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　必要に応じて [RADIUS] または [TACACS+] サーバ行を展開します。

ステップ 4　削除する認証サーバを右クリックし、[Remove Server] を選択します。

ステップ 5　メニュー バーで、[File] > [Deploy] の順に選択して、変更内容を DCNM-LAN サーバに適用します。

DCNM-LAN ローカル ユーザの表示

DCNM-LAN サーバのユーザ アカウントを表示するには、[Feature Selector] ペインで [DCNM Server Administration] > [DCNM Authentication Settings] の順に選択し、必要に応じて [Cisco DCNM Local Users] セクションを展開します。

[Contents] ペインに、DCNM-LAN サーバ ユーザ アカウント（ユーザ名と説明を含む）が表示されます。パスワードはセキュリティ保護のためマスクされて表示されます。表示される各フィールドの詳細については、「DCNM-LAN 認証設定のフィールドの説明」（P.15-13）を参照してください。

認証サーバ設定の確認

設定した特定の認証サーバを使用して、DCNM-LAN サーバがユーザを認証できることを確認できます。

手順の詳細

ステップ 1　[Feature Selector] ペインで、[DCNM Server Administration] > [DCNM Authentication Settings] の順に選択します。

ステップ 2　必要に応じて [Authentication Servers] セクションを展開します。

[Authentication Server Settings] の表には、RADIUS および TACACS+ サーバの設定が表示されます。

ステップ 3　[Verify] をクリックします。

[Verification] ダイアログボックスが表示されます。

ステップ 4　認証サーバ上の有効なユーザ アカウントのユーザ名とパスワードを入力します。

ステップ 5　確認する認証サーバの行の右にある [Verify] をクリックします。

DCNM-LAN クライアントに、確認が成功したか失敗したかを示すメッセージが表示されます。確認が失敗する場合、認証サーバが使用できないか、認証設定が正しくないことが考えられます。

DCNM-LAN 認証設定のフィールドの説明

ここでは、DCNM-LAN 認証設定機能における次の各フィールドについて説明します。

[Authentication Mode] セクション

表 15-3　[Authentication Mode] セクション

フィールド	説明
Local	DCNM-LAN がローカル ユーザ データベースだけを使用してユーザを認証するかどうか。
RADIUS	DCNM-LAN が RADIUS サーバを使用してユーザを認証するかどうか。設定されている RADIUS サーバが到達不能な場合、DCNM-LAN はローカル データベースを使用したユーザ認証にフォールバックします。
TACACS+	DCNM-LAN が TACACS+ サーバを使用してユーザを認証するかどうか。設定されている TACACS+ サーバが到達不能な場合、DCNM-LAN はローカル データベースを使用したユーザ認証にフォールバックします。

[DCNM-LAN Local Users] セクション

表 15-4　[DCNM-LAN Local Users] セクション

フィールド	説明
DCNM-LAN User Name	*表示のみ*。DCNM-LAN サーバ ユーザ アカウントの名前。この名前は、認証モードがローカルの場合か、現在の認証モードの認証サーバが到達不能である場合に、DCNM-LAN クライアントにログインするために使用できます。大文字と小文字は区別されます。すべての数字、記号、文字を使用できます。最小長は 1 文字、最大長は 198 文字です。
Full Name	ユーザ アカウントの他の名前（DCNM-LAN サーバ ユーザ アカウントを使用するユーザの名前など）。この名前は、DCNM-LAN クライアントにログインするときには使用できません。すべての数字、記号、文字を使用できます。最大長は 255 文字です。デフォルトでは、このフィールドはブランクです。
DCNM-LAN Role	ユーザ アカウントのロール。「ユーザ」または「管理者」のいずれかを指定できます。詳細については、表 15-1 を参照してください。デフォルトでは、DCNM-LAN サーバ ユーザ アカウントに User ロールが割り当てられます。
Password	DCNM-LAN サーバ ユーザのパスワード。このフィールドはセキュリティ保護のため、常にマスクされます。大文字と小文字は区別されます。すべての数字、記号、文字を使用できます。最小長は 1 文字、最大長は 255 文字です。

表 15-4　[DCNM-LAN Local Users] セクション （続き）

フィールド	説明
Description	DCNM-LAN サーバ ユーザの説明。すべての数字、記号、文字を使用できます。最大長は 255 文字です。デフォルトでは、このフィールドはブランクです。

[Authentication Servers] セクション

表 15-5　[Authentication Servers] セクション

フィールド	説明
Server Name	認証サーバの DNS 名または IPv4 アドレス。 • DNS 名：DNS 名を指定した場合、DCNM-LAN サーバがサーバの IP アドレスを解決できる必要があります。有効な DNS 名の文字は英数字です。 • IPv4 アドレス：IP アドレスを指定する場合、有効なエントリはドット付き 10 進表記です。
Secret Key	認証サーバの共有秘密キー。有効なエントリは、文字（大文字と小文字を区別）、数字、記号です。
Authentication Port	認証サーバが認証要求を待ち受ける TCP または UDP ポート番号。デフォルトでは、RADIUS サーバの認証ポートは UDP ポート 1812、TACACS+ サーバの認証ポートは TCP ポート 49 です。
Accounting Port	RADIUS 認証サーバが認証要求を待ち受ける UDP ポート番号。デフォルトでは、RADIUS サーバのアカウンティング ポートは UDP ポート 1813 です。
Authentication Method	DCNM-LAN サーバが、認証サーバへの認証要求で使用する認証プロトコル。サポートされる認証方式は次のとおりです。 • PAP • CHAP • MSCHAP • ASCII

その他の関連資料

DCNM-LAN 認証設定の管理に関する追加情報については、次を参照してください。

- 「関連資料」（P.15-15）
- 「標準」（P.15-15）

関連資料

関連項目	参照先
DCNM-LAN クライアントへのログイン	*「DCNM-LAN クライアントの起動」（P.14-8）*

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

DCNM-LAN 認証設定の機能の履歴

表 15-6 は、この機能のリリースの履歴です。

表 15-6　DCNM-LAN サーバ ユーザの機能の履歴

機能名	リリース	機能情報
DCNM-LAN 認証設定	5.0(2)	リリース 4.2 からの変更はありません。