管理者ガイド

Reflection for Secure IT

Windows Server

バージョン 7.2 SP1 Update1

〔 05版： 改訂日 2012年8月21日 〕

#JMN-00810I-0512H

目次

1. はじめに

1.1 適用

本マニュアルは、Reflection for Secure IT Windows Server 版（以後「RSIT Windows サーバ」と省略）バージョン 7.2 SP1 Upsate1 について、導入やその使用方法について解説したものです。
バージョン 7.2, 7.2 SP1 の参照マニュアルとしてもお使い頂けます。
導入後、デフォルト設定のままでもそのままお使い頂けますが、設定内容のセキュリティ上の効果をご理解頂き、お客様利用環境に適した正しい設定と運用を期待しています。
日本国内では北米ほど PKI 連携での使用が普及していない関係で、英文マニュアルにおける PKI や PKI Service Manager についての説明は割愛しました。必要時は、本社ドキュメントサイト <http://support.attachmate.com/manuals/rsit_win_server.html>上の英文マニュアルを参照下さい。

ファイル名/フォルダ名やプログラム表示名の中に会社名を含む場合があります。バージョンにより ″F-Secure″、″WRQ″、″Attachmate″ が使われていますが、F-Secure 社から WRQ 社への製品移管、WRQ 社 ⇒ AttachmateWRQ 社 ⇒ Attachmate 社 という会社名の変遷により旧社名が残っている事情からです。一貫した開発とサポートにより継続対応してまいりましたので、ご安心してご使用下さい。

1.2 SSH の概要

telnet によるリモートログインや FTP によるファイル転送等の平文による通信では、″盗聴″、″なりすまし″、″改ざん″といった不正行為を受ける危険性が存在します。SSH (Secure Shell)は、″暗号化″、″認証″、″データの完全性保証″により、これら悪意ある行為からパスワードや通信データを確実に保護します。

SSH はクライアント機能とサーバ機能で構成されます。クライアント側は、接続の起点となり、利用者に対しユーザインターフェースや各種コマンド、オプションを提供します。サーバ側は、常に待ち受けし、デーモンにより SSH 機能を完結するサービスを提供します。またサーバ側の設定内容(Configuration)により運用環境やクライアントからのアクセス制限等を指定します。

リモートからのターミナルログインが SSH の基本機能となります。さらに接続確立したセキュアな共通のセッションを利用し、リモートコマンド、scp(セキュアファイルコピー)、SFTP(セキュアファイル転送)、TCP ポート転送等の各種 SSH 標準機能を提供します。
リモートコマンドは、クライアント側で投入したコマンドをリモートホスト上で実行し、そのリターンコードで結果を判定します。
scp は 従来の rcp と類似のコマンド書式とオプションを用意し、rcp からの置き換えとして用意しました。

SFTP は、FTP と類似のコマンド、オプション、専用サブコマンドを用意し、FTP からの置き換えとして用意しました。
TCP ポート転送は TCP 上のアプリケーション通信をトネリングし、いわゆる VPN を実現します。

これら機能は、利用者が対話的にコマンド操作して利用するほかに、スクリプト/プログラム処理による自動実行を可能とし、お客様構築システムの組み込み部品として多く利用されています。

1.3 動作環境

(1) システム要件

(a) サポート OS

・Windows Server 2008 R2 (x86-64)　　… *<7.2 から追加対応>*、
・Windows Server 2008 (x86 および x86-64)、
・Windows Server 2003 (x86 および x86-64)、
・Microsoft Cluster Service に対応　　… *<7.2 から追加対応>*

注記：

①7.1 SP2 まで対応していた Windows Vista、Windows XP SP2、Windows 2000 Server SP4 が 7.2 から未サポートとなりました。
②Windows 同時使用ユーザ数/接続クライアント数等のライセンス契約は遵守下さい。
③動作条件とは別に、Windows の脆弱性対策の観点から、常に最新の SP(サービスパック) ならびに アップデートを適用しておくことを強く推奨します。

(b) サポート CPU

・x86 (32bit)、・x86-64 (64bit AMD x64, 64bit EM64T)
(インストールプログラムファイルには、32 ビット版と 64 ビット版があります。)

(c) 必要プログラム

・マイクロソフト XML 6.0 parser
インストール時に存在しない場合、セットアッププログラムが自動的にインストールします。

2. 導入

2.1 導入前の確認事項

(1) インストールプログラムファイル

(a) SP(サービスパック)の扱い

バージョン 7.2 SP1 は バージョン 7.2 の SP(サービスパック)版ですが、7.2 SP1 を新規に導入する際は、事前に 7.2 をインストールする必要はなく、最初から 7.2 SP1 をインストールすることで全ての導入が完結します。

(b) CPU への対応

32 ビット版と 64 ビット版があります。導入 OS に応じて使い分けします。

RSIT バージョン	OS ビット幅	インストールプログラムファイル名
7.2 SP1	64 ビット版	rsitservwin-7.2.1.736-wx64.exe
	32 ビット版	rsitservwin-7.2.1.736-w32.exe
7.2	64 ビット版	rsitservwin-7.2.151-wx64.exe
	32 ビット版	rsitservwin-7.2.151-w32.exe

(2) Windows Server OS の再起動

RSIT Windows サーバプログラムをインストールした後に Windows OS の再起動が必要です。

(3) インストール操作ユーザ

ローカル Administrator アカウントから必ずインストールします。

(4) バージョンアップ時の旧バージョンの処理 (2.2 項 で詳述)

旧バージョンが RSIT Windows サーバ 6.0 以降の場合、旧バージョンをアンインストールせずにそのまま 7.2 SP1 を追加インストールします。既にアンインストール済みでも問題はありませんので、その場合は新規インストールして下さい。

旧バージョンが F-Secure SSH Windows サーバ 5.3 以前の場合は、sshd2_config ファイルを保管した上で、F-Secure SSH Windows サーバを事前にアンインストールして下さい。

2.2 導入上のポイント

新規インストールとバージョンアップ時の手順について説明します。

RSIT Windows サーバ では、バージョン 7.1 以降 上書きインストール時に旧バージョンの設定内容を自動移行する機能が追加されました。よって本章(=２章)で示すバージョンアップ手順は、旧バージョンの設定内容を自動移行するように、旧バージョンはアンインストールせずにそのままとして新バージョンを追加インストールする手順を標準として説明します。旧バージョンを一旦アンインストールし、改めて新バージョンを新規インストールする手順でも問題はありません。

また、旧バージョンの対象は RSIT Windows サーバ 6.0 以降とし、F-Secure SSH Windows サーバ 5.3 以前は対象外としました。F-Secure SSH Windows サーバからバージョンアップする時には、参照用に従来の sshd2_config ファイルを保存の上で旧バージョンをアンインストールし、改

めて 7.2 SP1 を新規インストールして下さい。
手順説明の前に、仕様/動作上のポイントを示します。

(1) 関連ファイルのインストール先と名称（デフォルト時）

	Ver	
プログラム インストール先フォルダ	7.x	C:¥Program Files¥Attachmate¥RSecureServer
	6.x	C:¥Program Files¥F-Secure¥ssh server
関連ファイル (設定ファイル,ホスト鍵) の 保存先フォルダと ファイル名	7.x	1) Windows Server 2008 の場合 C:¥ProgramData¥Attachmate¥RSecureServer¥ 2) Windows Server 2003 の場合 C:¥Documents and Settings¥All Users¥Application Data ¥Attachmate¥RSecureServer
		・設定ファイル： rsshd_config.xml ・ホスト鍵　　： hostkey/ hostkey.pub
	6.x	C:¥Program Files¥F-Secure¥ssh server
		・設定ファイル： sshd2_config ・ホスト鍵　　： hostkey/ hostkey.pub

(2) バージョンアップ時の 旧 Ver 7.x/6.x の処理比較

	旧 Ver が 7.x の場合	旧 Ver が 6.x の場合
検知 旧 Ver の削除	自動アンインストールする	アンインストールしない
旧 Ver 検知時の 新 Ver インストール先	インストール時の指定インストール先	
	注記： 旧 Ver のインストール先情報を引き継がないため、旧 Ver 同様に今回もデフォルトから変える場合は、インストール時に明示的に指定するが必要あります。	**注記**: Ver6.x と 7.x のインストール先は上記表のように全く別になります。
追加インストール終了後の OS 再起動後の sshd サービスの開始	7.2 SP1 sshd サービスを自動開始	旧 Ver 6.x sshd サービスか 7.2 SP1 sshd サービスのいずれかを開始 [注 1]

[注 1]
旧 Ver 6.x はアンインストールされず存在し自動開始設定のままなので、インストール完了後の Windows OS 再起動時には、新旧両方とも sshd サービスを開始しようとします。しかし実際は、開始の遅かった方が、同一リスニングポートが既に使われているということで停止するため、新旧いずれもか片方の sshd サービスが稼働し、もう一方が停止状態になります。まずは、手操作でいずれも停止させ、設定内容を確認して下さい。同時動作以外は、いずれのサービスも手操作で停止/開始が可能です。

sshd サービス稼動状況の確認方法

a)設定画面を開き、設定画面上のステータス表示で確認

b)Windows タスクマネージャによるプロセス確認：

Ver 7.x プロセス	rsshd.exe
Ver 6.x プロセス	fsshd2.exe

(3) インストール手順の概要

概要は以下のようになります。

	新規インストール	バージョンアップ	
		7.x から	6.x から
①	・7.2 SP1 のインストール（詳細手順は 2.3 参照）		
②	・Windows OS を再起動		
③	・手操作で sshd サービスを停止		手操作で sshd サービスを停止 〈前述(2)[注 1]参照〉
④	・7.2 SP1 設定画面より設定操作と内容確認		
⑤	・手操作で 7.2 SP1 sshd サービスを再起動（OS の再起動は不要）		
⑥	・動作確認		
⑦	—		6.x をアンインストール

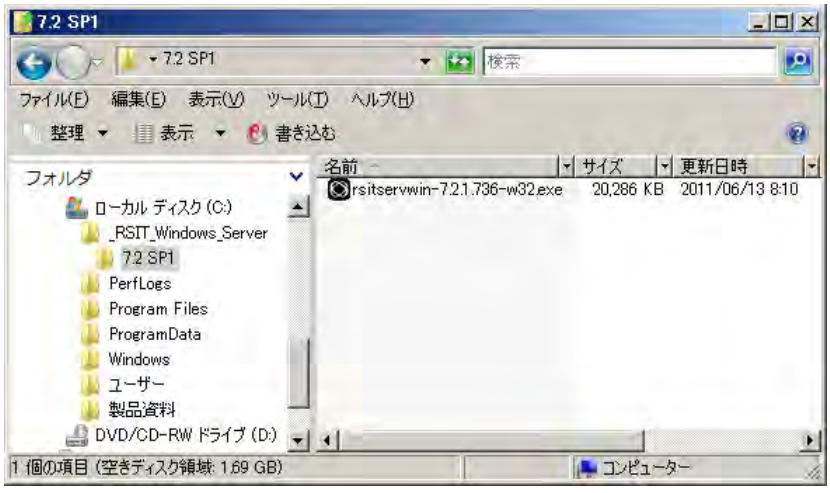
2.3 インストール操作詳細手順

ここではインストールプログラムファイルを直接起動した時の操作手順について説明します。

製品 CD を用いて導入する場合は、起動と解凍処理がスキップされ(3)から開始します。

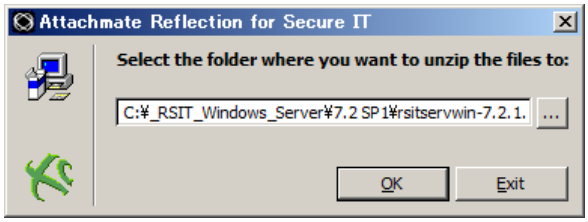
(1) インストールプログラムファイルの実行開始

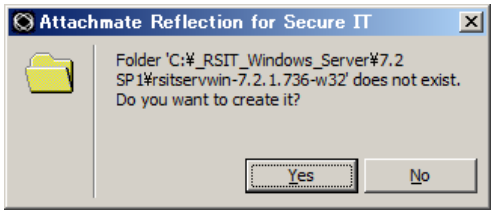
インストールプログラムファイル(例えば rsitservwin-7.2.1.736-w32.exe)をローカルディスク上の任意のフォルダ下に置き、起動します。



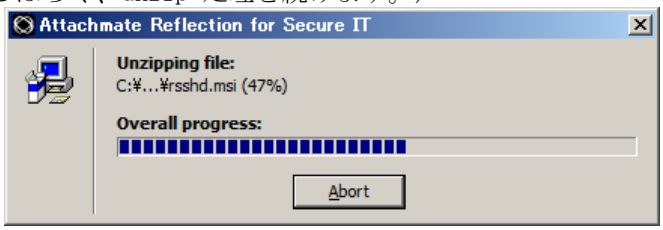
(2) インストールプログラムファイルの unzip 処理

unzip 先の確認画面を表示します。インストールプログラムファイルと同一の場所に同一名称の新規フォルダ作成の確認画面を表示しますので、そのまま[OK]ボタンをクリックし、次画面で[Yes] ボタンをクリックします。





(しばらく、unzip 処理を続けます。)



(3) 開始画面の表示 〈製品 CD からインストールする場合は、この開始画面から始まります。〉

a) Microsoft XML 6.0 parser が存在しない場合：**〈画面 A〉**

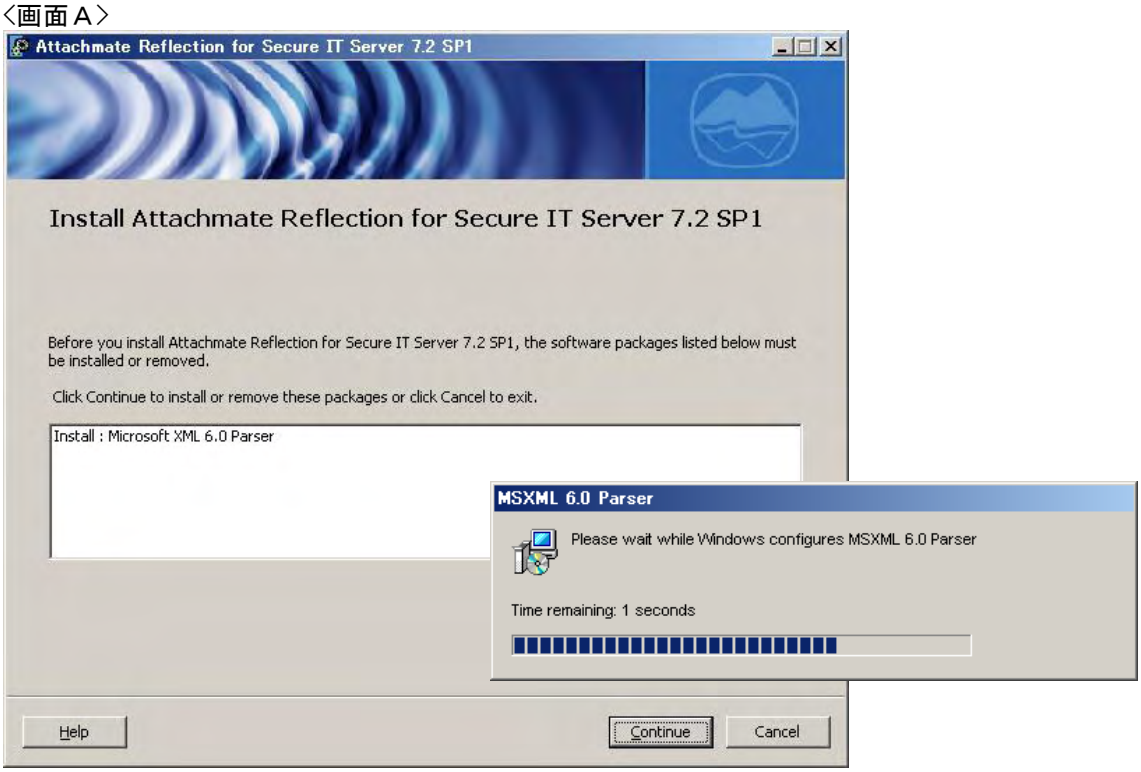
Microsoft XML 6.0 parser の導入を開始しますので、[Continue]ボタンをクリックし、処理を継続します。

b) Microsoft XML 6.0 parser が存在する場合：

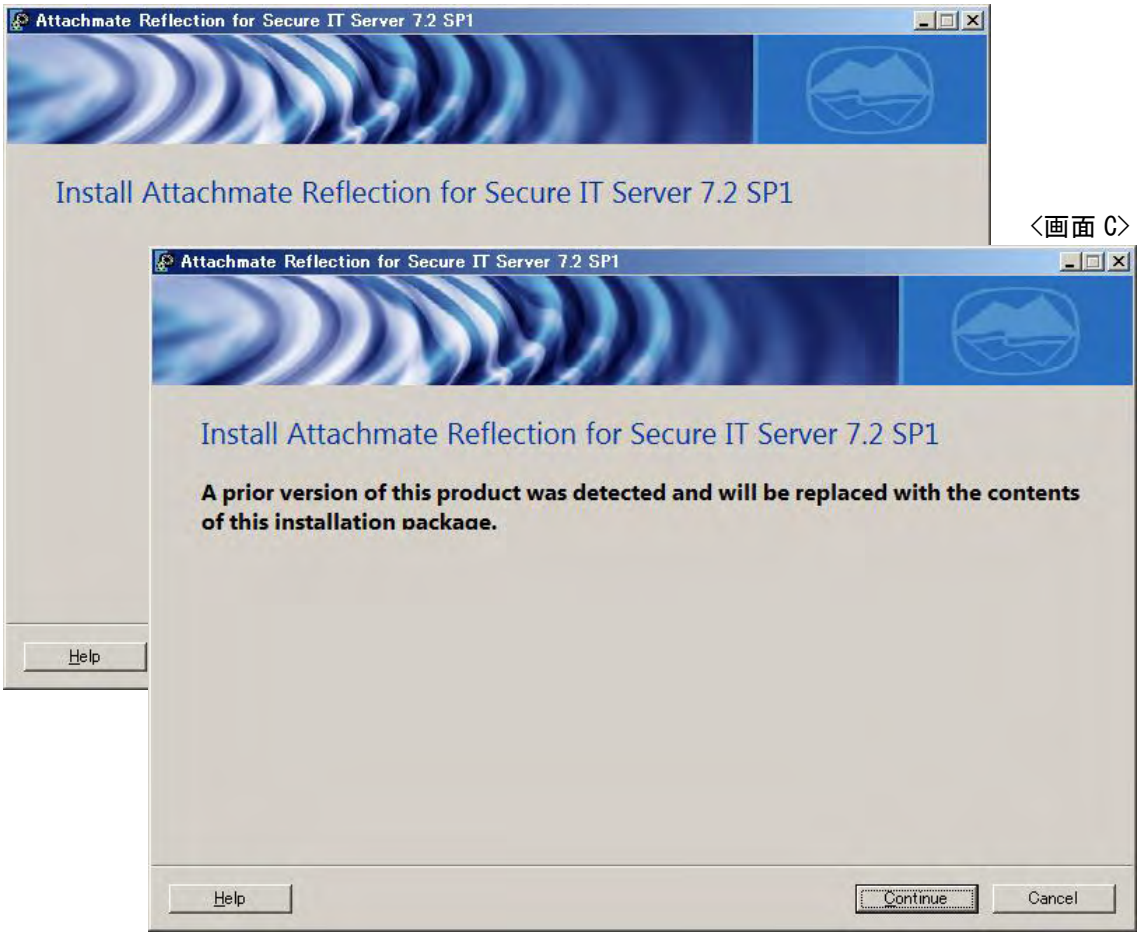
[Continue]ボタンをクリックし、処理を継続します。

バージョン 7.x からのバージョンアップ時には、画面上に旧バージョン 7.x を検知した旨を英文で表示します。**〈画面 C〉**

〈画面Ａ〉


Attachmate Reflection for Secure IT Server 7.2 SP1
Install Attachmate Reflection for Secure IT Server 7.2 SP1
Before you install Attachmate Reflection for Secure IT Server 7.2 SP1, the software packages listed below must be installed or removed.
Click Continue to install or remove these packages or click Cancel to exit.
Install : Microsoft XML 6.0 Parser
MSXML 6.0 Parser
Please wait while Windows configures MSXML 6.0 Parser
Time remaining: 1 seconds
Help
Continue
Cancel

〈画面Ｂ〉

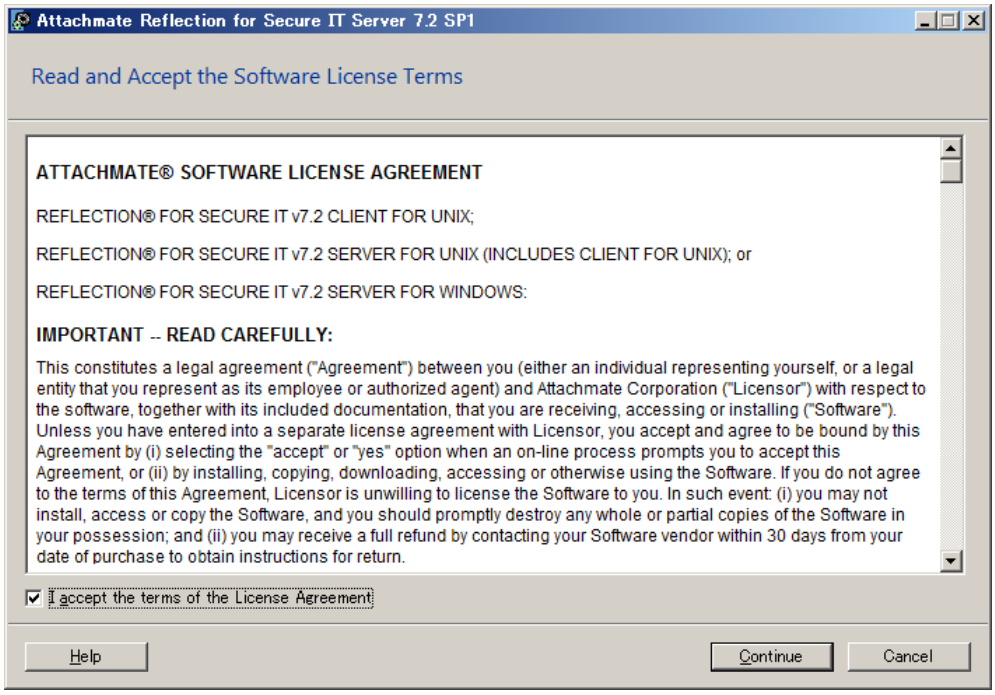

Attachmate Reflection for Secure IT Server 7.2 SP1
Install Attachmate Reflection for Secure IT Server 7.2 SP1
Help

〈画面Ｃ〉

Attachmate Reflection for Secure IT Server 7.2 SP1
Install Attachmate Reflection for Secure IT Server 7.2 SP1
A prior version of this product was detected and will be replaced with the contents of this installation package.
Help
Continue
Cancel

(4) Software License Agreement(ソフトウェア使用許諾契約書)画面の表示

内容を確認し、チェックマークを入れ、 [Continue]ボタンをクリックします。



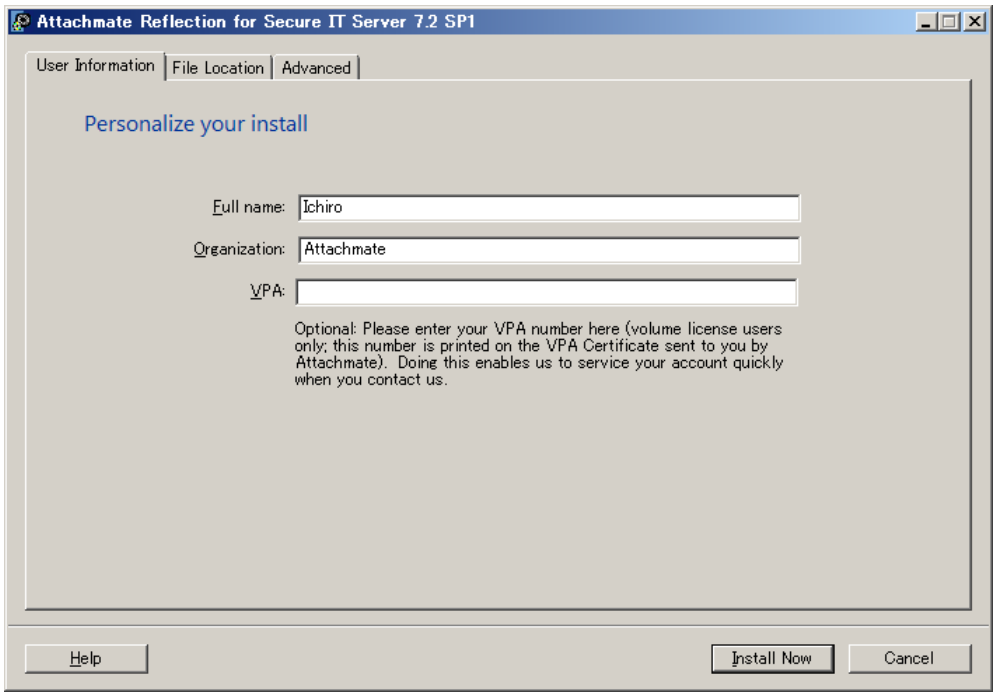
(5) インストール情報の入力

インストール時に指定する全ての情報を３つのタブ画面より入力し、情報入力後に、[Install Now]ボタンをクリックします。

何も入力せずに[Install Now]ボタンをクリックしても処理は正常に継続します。

(5-1) [User Information]タブ画面からの入力

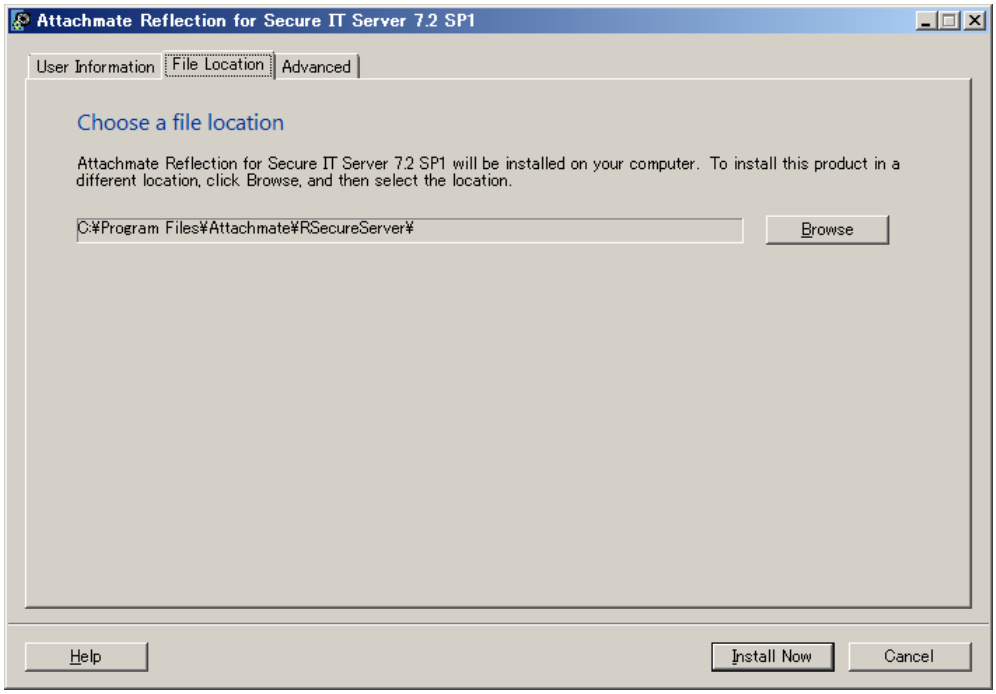
必要なお客様情報を入力します。



(5-2) [File Location] タブ画面からの入力

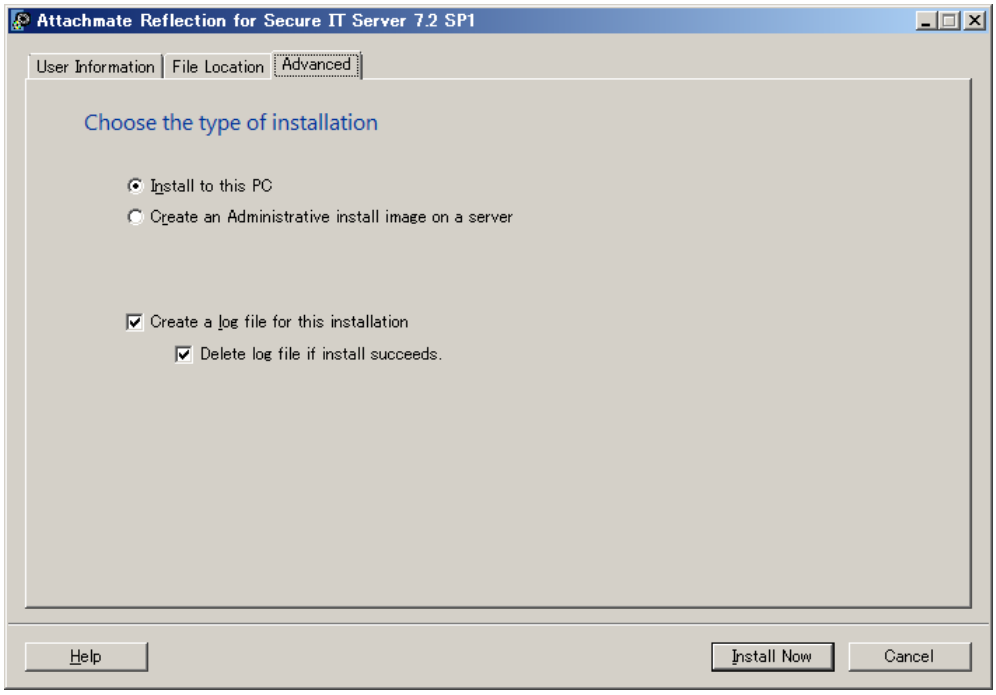
インストール先を指定します。

デフォルトは、欄内に表示しているインストール先です。



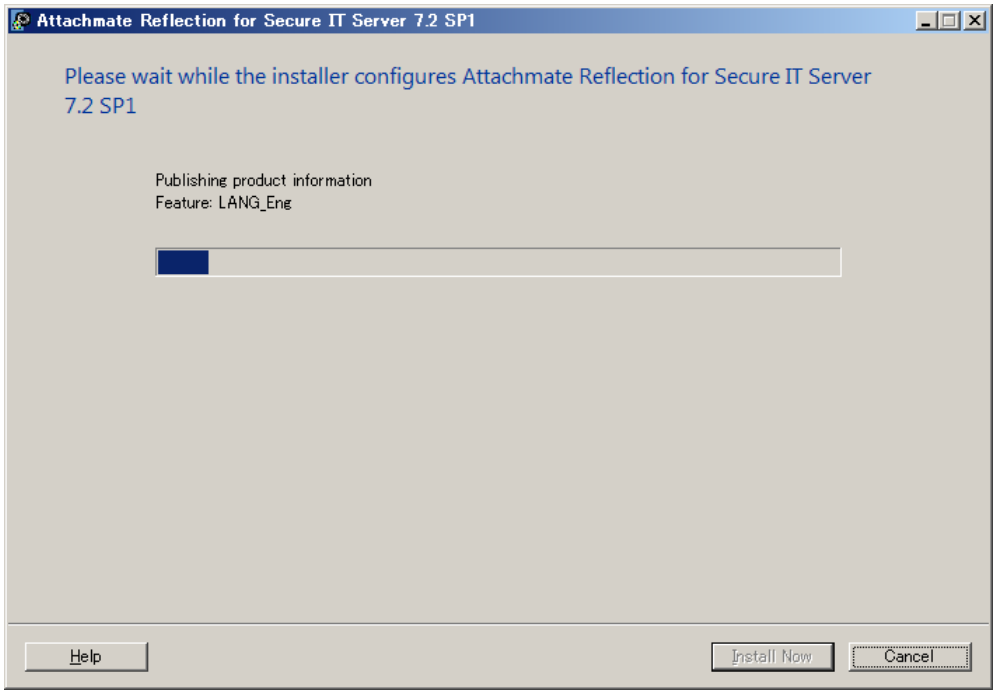
(5-3) [Advanced]タブ画面からの入力

本画面内の設定は、原則そのままとします。



(6) インストール処理の進行表示

処理中ですので、次の完了画面を表示するまで、しばらく待ちます。

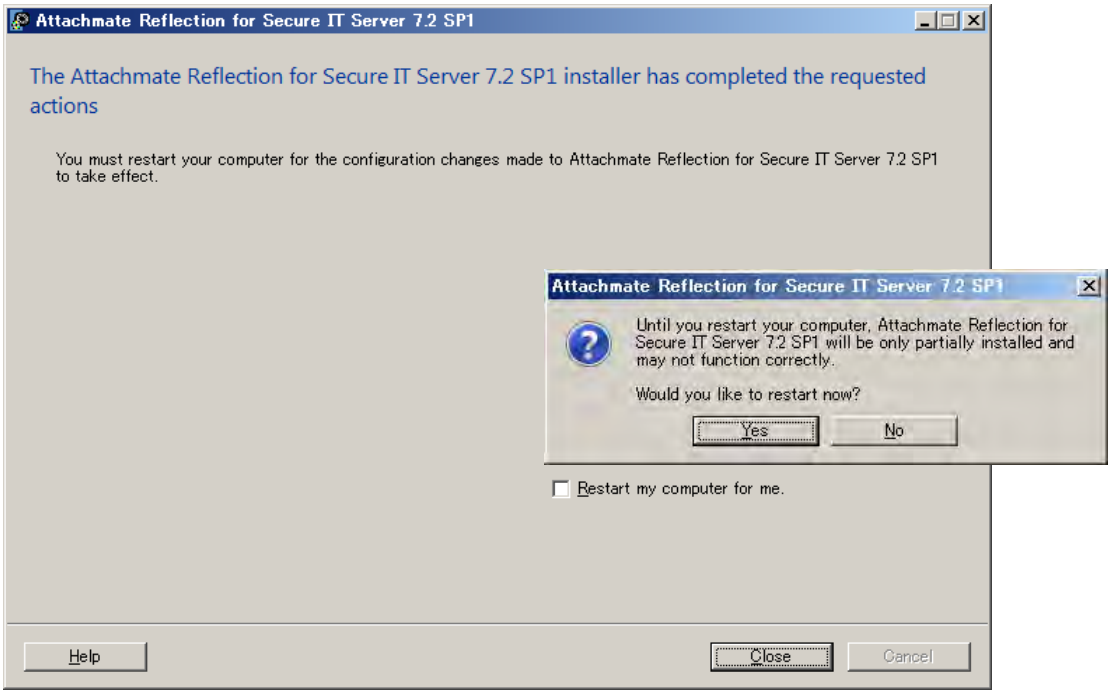


(7) インストール完了画面の表示

インストールが完了しました。Windows OS を再起動します。

"Restart my computer for me." にチェックマークを入れるか、入れずに[Close]ボタンをクリックし、OS 再起動確認画面で[Yes]ボタンをクリックすることで、OS が再起動します。

OS 再起動確認画面で[No]ボタンクリック時は、OS の再起動処理へは移行せずにインストール作業を終了します。正しく使用頂くためには、必ず OS の再起動をお願いします。



(8) OS 再起動後の確認と操作

OS 再起動後、sshd サービスは自動的に開始します。

GUI 設定画面を開き、手操作にて sshd サービスを停止し(「3. 操作」参照)、GUI 設定画面を通じてコンフィグの指定とその内容確認をします。

設定内容を確認したら、手操作にて sshd サービスを再開します。

2.4 アンインストール

(1) アンインストール操作

アンインストールは、Windows の「プログラムの追加と削除」/「プログラムと機能」から実施します。アンインストールにより、プログラムファイルは完全に削除されますが、設定ファイルとホスト鍵は削除されずに残ります。

旧バージョン 6.x をアンインストールせずに新バージョン 7.x をそのまま追加インストールした場合は、両方存在することになります。旧バージョン 6.x をアンインストールする時には、「プログラムの追加と削除」/「プログラムと機能」上の下記名称を確認し削除下さい。

バージョン 7.2 SP1	Attachmate Reflection for Secure IT Server 7.2 SP1	次頁〈図 A〉
バージョン 6.x	WRQ Reflection for Secure IT Server	次頁〈図 B〉

〈図Ａ〉　バージョン 7.2 SP1

〈図Ｂ〉　バージョン 6.x

3. 操作

3.1 設定画面からの操作設定

(1) 設定画面の表示

画面左下 Windows の [スタート]ボタンから、

[スタート] > [すべてのプログラム] > [Attachmate Reflection]
> [Reflection SSH Secure Configuration]

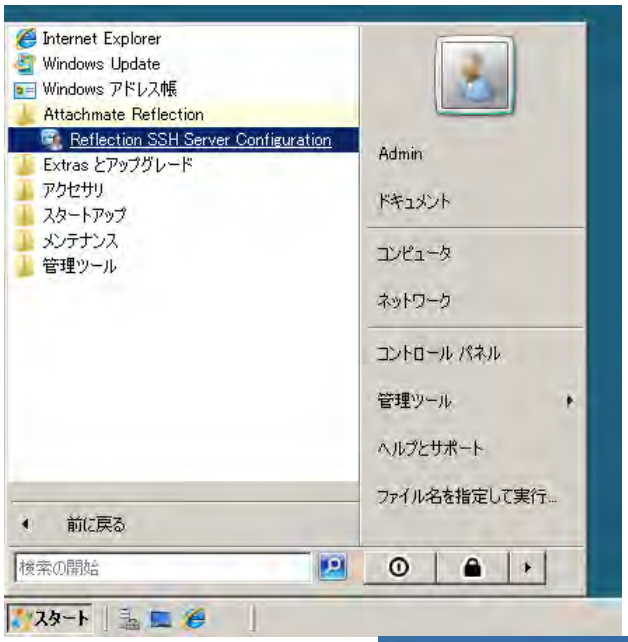
と順次選択し設定画面を表示します。

注記：

設定画面の表示動作と sshd のサービス稼動とは独立した別プロセスです。

設定画面の表示：sshconsole.exe　sshd サービス：rsshd.exe

〈Windows Server 2008 の場合〉



〈Windows Server 2003 の場合〉

(2) 設定画面の構成

設定画面は大きく次の部位から構成されています。

部位	内容
メニュー	File、View、Action、Help の下に各種個別の指定があります。 ・File > Save Settings, Close ・View > Toolbar, Event Viewer, Latest Debug log File ・Action > Start Server, Stop Server, Restart Server, Configure Cluster, Restore All Default Settings, Restore Pane Defaults ・Help > Help Topics, Support Web, About Reflection
操作用ボタン	  ・左から [Save Settings], [Event Viewer], [Latest debug log file] … *<7.2 SP1 から追加>*, [Start], [Stop], [Restart] ・右上に [Restore Pane Defaults]ボタン
[Status] タブ画面	・sshd サービスの状態を表示 ・RSIT Windows サーバの バージョン/ build とインストール先を表示
[Identity] タブ画面	・RSIT Windows サーバ ホスト鍵情報(所在, コメント, ダイジェスト)の表示 ・RSIT Windows サーバホスト証明書情報 ・Server version string (アクセス開始時にクライアントへ提示の自己情報)
[Configuration] タブ画面	・各種設定の指定/表示画面 (4. 設定 を参照)

(3) 設定画面上の基本操作

a) sshd サービスの開始と停止

設定画面上のボタン操作かメニューの選択により、sshd サービスの開始/停止/再起動 が可能です。

b) 設定内容の保存と反映

[Configuration]タブ画面内の各種設定画面上で入力編集の後、[Save Settings] ボタン/メニューの選択によりその内容を"rsshd_config.xml"ファイルに上書き保存します。上書き保存後にクライアント接続があったものから設定内容従った sshd サービスの動作になります。

c) 設定内容のデフォルト値への変更

[Restore Pane Defaults] ボタン/メニューの選択 ⇒ 表示画面内容をデフォルト値へ

[Restore All Default Settings]メニューの選択 ⇒ 全画面内容をデフォルト値へ

画面内容をデフォルト値に戻した後に、[Save Settings]ボタン/メニューの選択によりその内容を"rsshd_config.xml"ファイルに上書き保存します。上書き保存後にクライアント接続があったものから設定内容に従った sshd サービスの動作になります。

4. 設定

4.1 基本事項とその設定

デフォルト設定内容の状態でも、高いセキュリティ水準での運用が可能ですが、「4.2 設定詳細」の内容を理解され、お客様セキュリティポリシー運用方針に従った適切な設定をされ運用開始されることを推奨致します。

そのため「2.2 導入上のポイント (3)導入の流れ」④における設定と内容確認をします。

4.2 設定詳細

RSIT Windows サーバでは、全ての設定を GUI 設定画面から指定し、全て"rsshd_config.xml"ファイルに保存されます。

"rsshd_config.xml"ファイルの所在はデフォルトでは下記ディレクトリ下ですが、バージョン 7.2 から保存先をメニュー操作(Action > Set Data Folder) から変更可能になりました。

a) Windows Vista, Windows Server 2008 の場合:

C:¥ProgramData¥Attachmate¥RSecureServer¥rsshd_config.xml

b) Windows XP, Windows Server 2003 の場合:

C:¥Documents and Settings¥all users¥Application Data¥Attachmate¥RSecureServer ¥rsshd_config.xml

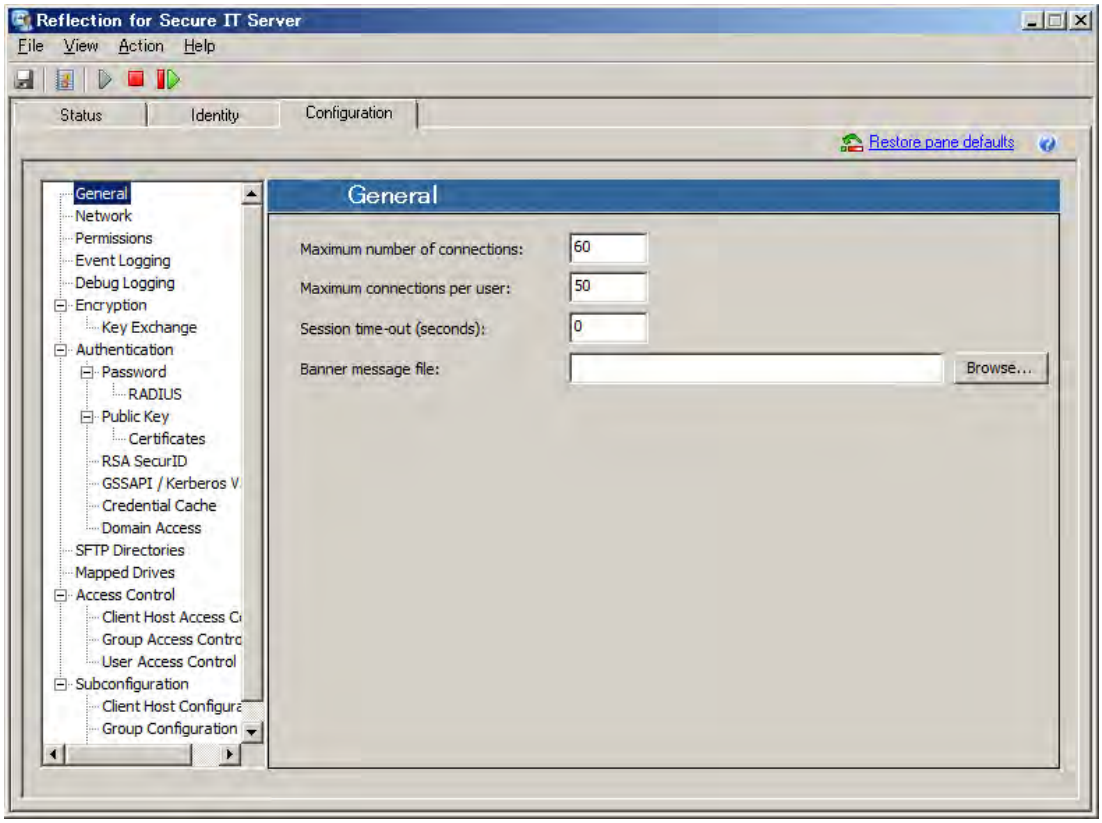
注記:

バージョン 6.1 以前と違い、全ての設定内容が GUI 設定画面を通じて設定可能となり、かつ 保存ファイルがテキストファイルでなく xml ファイルとなりました。直接 xml ファイルを編集することは思わぬエラーの原因ともなりますので、禁止とします。

以下、設定画面毎にその設定内容について説明します。

[Configuration] タブを選択し、画面左欄内のツリー状の選択メニューから対象設定画面名称を選択し表示させます。

4.2.1 ［Genaral］設定画面



[Maximum number of connections:]

サーバに同時に接続可能な接続数の上限を設定します。

デフォルト値は ″60″。値″0″ は無制限を意味します。無制限指定時は、OS のリソース等の別の要因による制限に注意下さい。

セッション Reuse 動作時は、チャネル多重されても connection の数は１とカウントします。

[Maximum connections per user:]

１ユーザ当たりの同時接続数の上限を設定します。値″0″ は無制限を意味します。

connection reuse（既存確立セッション相乗り）の場合は１connection としてカウントします。

[Session time-out (seconds):]

データが送受信されていないアイドル状態が継続した時に、指定時間経過後に接続を自動切断します。その指定時間を秒単位で入力します。

値″0″の場合、機能無効となります。

[Banner message file:]

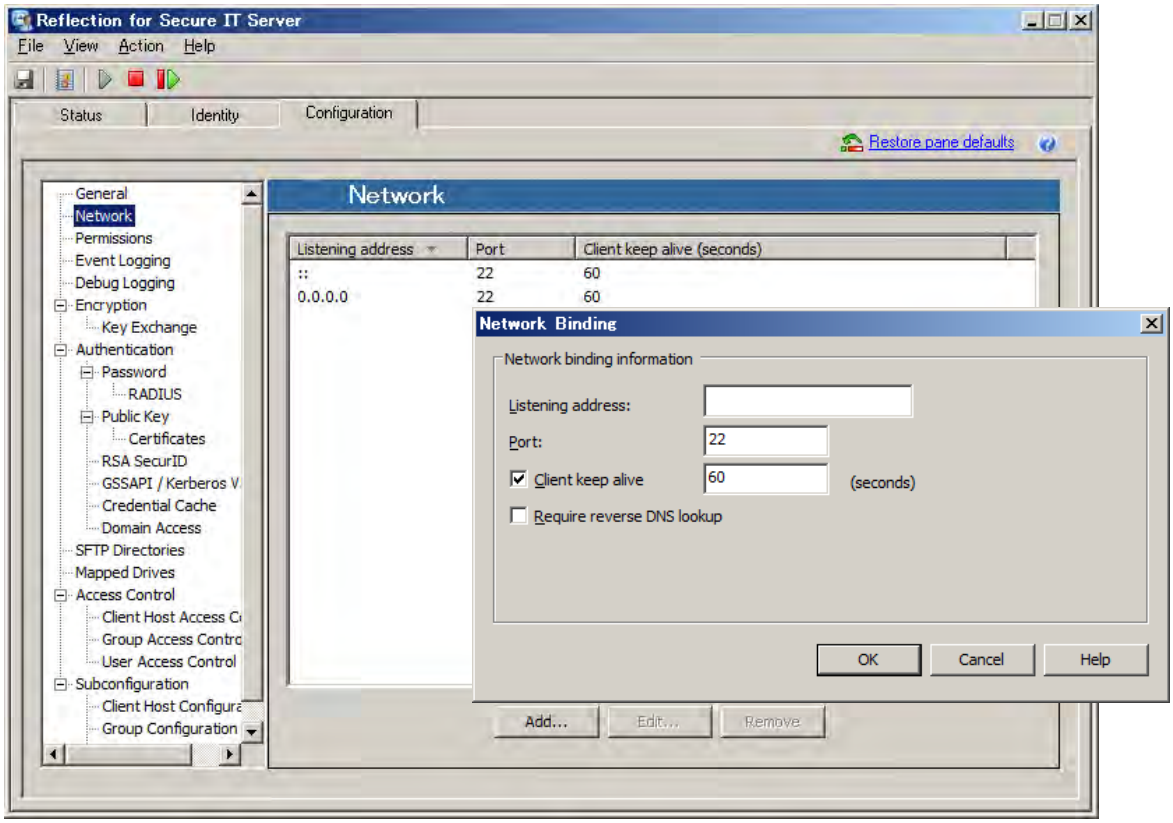
接続開始時にクライアント側に追加で表示するメッセージテキストファイルを指定します。

ファイルの文字コードは UTF-8 を使用し、それ以外の文字コードの時には自動変換されます。

注記：

SSH クライアントによっては、バナー表示に未対応のものがあります。接続クライアントが本機能に全て対応していることを確認の上で指定下さい。

4.2.2 ［Network］設定画面



sshd サービスが待ち受け(Listening)するアダプタとポート番号の表示と指定をします。
デフォルトは、全ての有効アダプタに対してポート 22 番を割り当てます。設定変更する場合は、[Add]/[Edit]ボタンをクリックし、[Network Binding]ダイアログボックスを通じて指定します。

[Network Binding]ダイアログボックス：

[Listening address:]

SSH クライアントからの接続を待ち受けするアダプタ(ポート)の IP アドレスを指定します。
デフォルトでは、全ての有効な IP アドレスからの受信が有効です。
全 IP アドレス指定は、IPv6 の場合 "::"とし、IPv4 の場合 "0.0.0.0" とします。

[Port:]

SSH クライアントからの接続を待ち受けする TCP ポート番号を指定します。
デフォルトは ポート 22 番です。

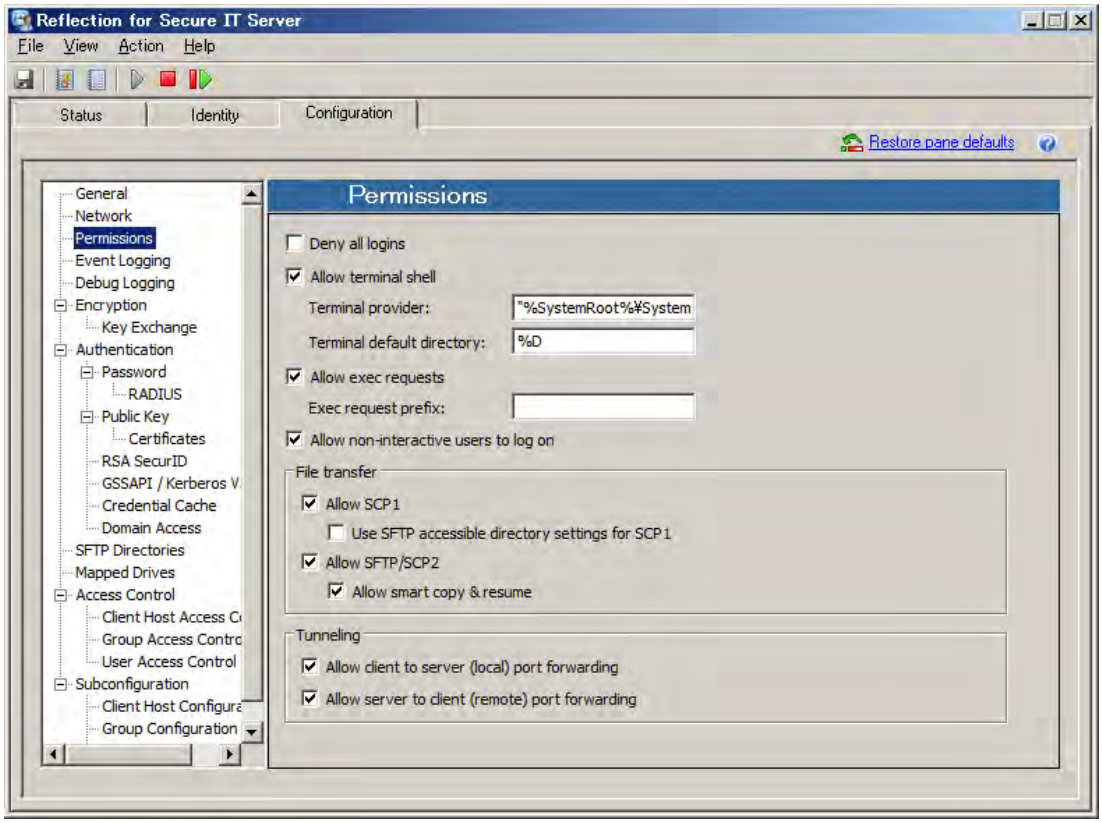
[Client keep alive]

クライアント側に対して正常性監視をします。キープアライブパケットに対して指定時間応答が無い場合に切断します。デフォルトは 60 秒 です。

[Require reverse DNS lookup]

接続要求開始時に、IP アドレスからドメイン名を得るために DNS の逆引きの動作をするかの指定をします。指定時に逆引きに失敗した時は、ユーザ認証処理を中断しすぐに切断します。

4.2.3 [Permissions] 設定画面



各種 SSH サーバサービスの提供有無をサーバ共通に設定します。

本設定の他、[Subconfiguration] 設定により、ほぼ同一内容を Client Host/Group/User 個別に指定可能です。

[Deny all logins]

(現在既に確立している接続以外の、今後の新たな)クライアントからの接続を全て拒否する指定です。[Subconfiguration]の指定に本設定はありません。

[Allow terminal shell]

クライアントからのターミナル接続を許可するかどうかの指定です。

注記：

ターミナル接続動作許可決定要因として、Windows OS のセキュリティ設定内容も影響します。

[Terminal provider:]

ターミナル接続動作に対応するサーバ側実行プログラムを指定します。

デフォルトは Windows 標準の cmd.exe です。指定変更時は、絶対パスで指定します。

注記：

指定時にパス名にスペースを含む場合は、Windows のセキュリティ上、ダブルクウォーテーション(″ ″)で囲って下さい。

[Terminal default directory:]

ターミナル接続開始時のカレントディレクトリとなるパス指定をします。

パス指定または、パターンストリング("%D","%H",%u","%U")を使用可能です。

デフォルトは "%D"(Windows ユーザプロファイル) 先です。

Windows ユーザプロファイルデフォルト値は以下の通りです。(管理者権限ユーザにより変更可)

a) Windows XP, Windows Server 2003 の場合:

C:¥Documents and Settings¥username¥

b) Windows Vista, Windows Server 2008 の場合:

C:¥Users¥username¥ (オブジェクト名"C:¥Users"、表示は"C:¥ユーザー")

〈パターンストリング〉

・%D：ユーザプロファイルフォルダ

・%H：ユーザホームフォルダ

・%u：ユーザログイン名

・%U：ドメインユーザログイン名 (domain.username の書式)

[Allow exec requests]

SSH リモートコマンドを実行可能とするかどうかを指定します。

デフォルトは実行可状態です。

[Allow non-interactive users to log on]

Windows サーバ OS の ローカルセキュリティポリシー設定にて、"ローカルログオンを許可する" 対象になっていないユーザ/グループに対して、SSH ログインを許可するかどうかを指定します。

注記：

Windows Server 2003 の場合は、"ローカルログオンを許可する" 対象になっていないユーザ/グループに対しては、コマンドプロンプトが使用できない結果 SSH ログインが失敗し、実質的にローカルセキュリティポリシーの指定と同一の動作になります。

File transfer

[Allow SCP1]

OpenSSH の scp（ここでは"SCP1"と表記）は 標準仕様に準拠しない非sftpプロトコルを使用しています。RSIT Windows サーバでは、この非 sftp プロトコルにも対応しました。
本指定は OpenSSH クライアントからの scp に対応するかどうかの指定をします。
デフォルト状態では対応します。

注記：

OpenSSH の scp はSSHセッション内の1チャネルを介したrcpコマンドにて実現しています。よって、本設定からチェックマークを外し対応不可とした場合でも、[Allow exec requests]にて実行可能の設定をしている場合は、OpenSSH からの scp が可能な状態になります。

[Use SFTP accessible directory settings for SCP1]

OpenSSH からの scp 動作に対し、[SFTP Directories]設定画面内の設定内容を適用するかどうかを指定します。

[Allow SFTP/SCP2]

クライアントからの sftp 及び（標準仕様に準拠した sftp プロトコルによる）scp（ここでは"SCP2"と表記)を許可するかどうかを指定します。デフォルトは、許可状態です。

[Allow smart copy & resume]　　*…〈7.2 SP1 から追加〉*

Smart Copy 機能(=同一ファイル存在時に転送処理をスキップする機能)と Resume 機能(=リトライ時に前回途中まで転送した分の次から再開する機能)の有効/無効を指定します。
デフォルトは有効状態です。

注記：

SSH クライアント側で Smart Copy 機能と Resume 機能に未対応の場合は、本設定に関係なく動作は無効になります。

Tunneling

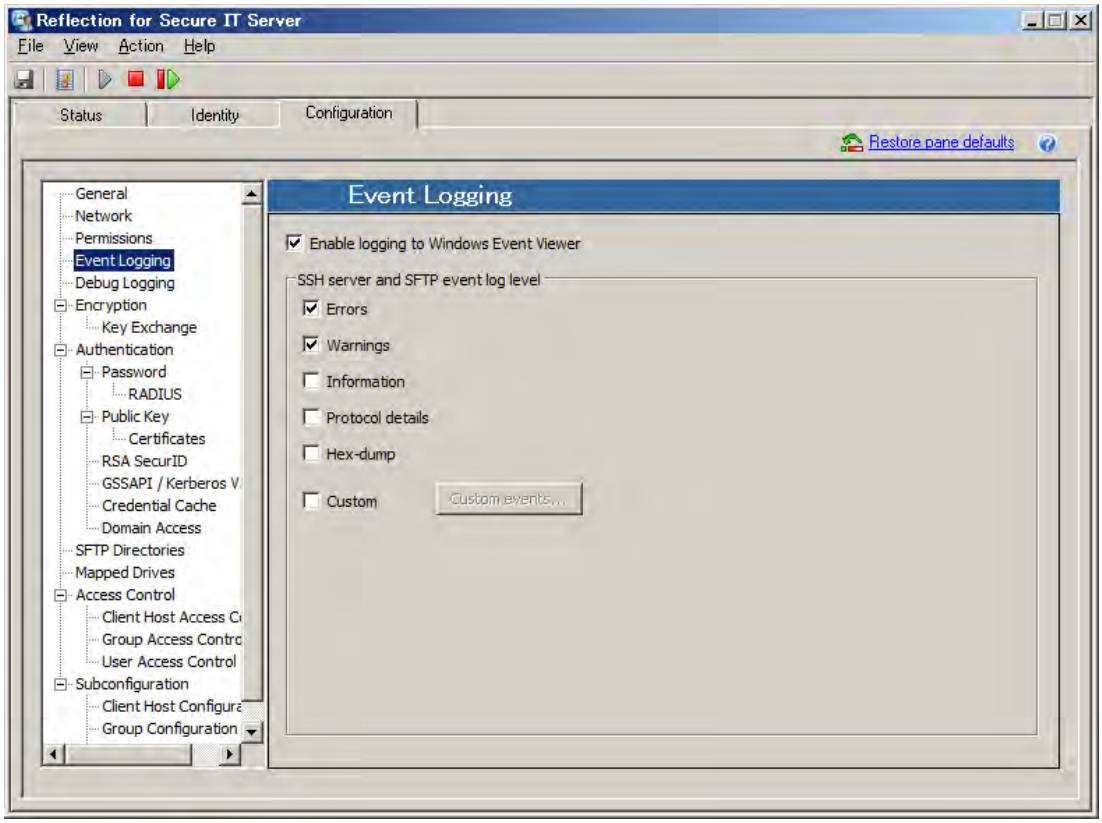
[Allow client to server (local) port forwarding]

クライアントからの "ローカル TCP ポート転送" を許可するかどうかを指定します。

[Allow server to client (remote) port forwarding]

クライアントからの "リモート TCP ポート転送" を許可するかどうかを指定します。

4.2.4 [Event Logging] 設定画面



Windows イベントログへの記録動作の指定をします。

[Enable logging to Windows Event Viewer]

イベントログへの記録を有効にします。

[Errors], [Warnings], [Information], [Protocol details], [Hex-dump]

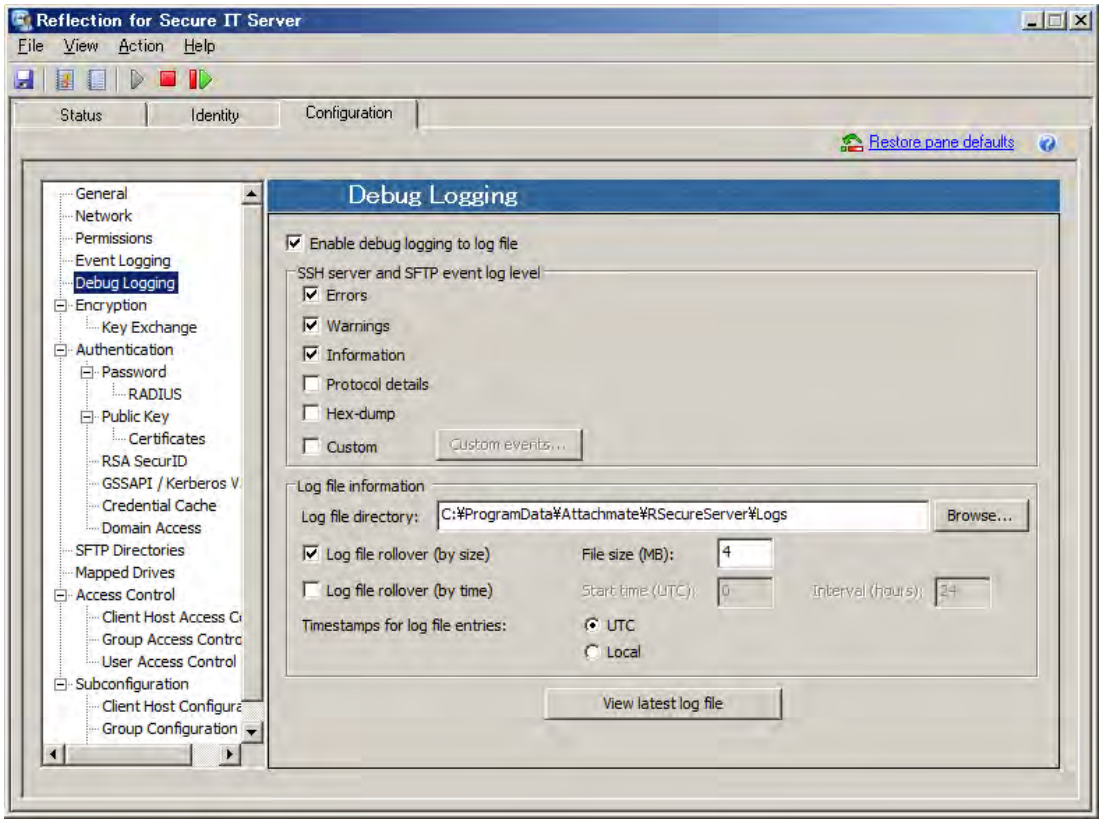
チェックマークを入れることで、どのレベルまで記録するかを指定します。

下に行くほどより詳細になります。チェックを入れた項目の上位は無条件にチェックマークが入ります。デフォルトは、"Errors", "Warnings" レベルを記録します。

[Custom]

チェックマークを入れ、[Custom events]ボタンをクリックすることで、個々の詳細イベントを個別に指定可能です。

4.2.5 [Debug Logging] 設定画面



RSIT Windows サーバ専用のデバッグログ採取の指定をします。

デバッグログは問題解析用です。特にクライアントとの接続失敗時に有効な情報を提供します。

メッセージを出力しながらプログラム処理をする関係で、RSIT Windows サーバの本来の処理の処理速度は低下します。通常運用ではチェックマークを外し無効にしてお使い下さい。

[Enable debug logging to log file]

デバッグログの記録を有効にします。

有効時、SSH サーバのサービスを起動する毎に別名の新たなデバッグログファイルを生成します。

[Errors], [Warnings], [Information], [Protocol details], [Hex-dump]

チェックマークを入れることで、どのレベルまで記録するかを指定します。

下に行くほどより詳細になります。チェックを入れた項目の上位は無条件にチェックマークが入ります。

[Custom]

チェックマークを入れ、[Custom events]ボタンをクリックすることで、個々の詳細イベントを個別に指定可能です。

Log file information

[Log file directory]

デバッグログを生成するディレクトリ先を指定します。

デバッグログは指定ディレクトリ下に、"RSSHD-YYYYMMDD-HHMMSSmmm.log"というファイル名で作成されます。ここで、"YYYYMMDD-HHMMSSmmm"は、開始時刻を示し、"YYYYMMDD" は年月日、"HHMMSSmmm" は 時分秒+マイクロ秒 です。

[Log file rollover (by size)]

上限ファイルサイズを指定し、そのサイズに達したら現デバッグログファイルを完了し、新ログファイルを新たに生成し切り替えます。

指定サイズは１ファイルのサイズ指定であり、全ログファイル容量は増え続けますので注意下さい。

[Log file rollover (by time)]

指定時間間隔で出力デバッグログファイルを新規に生成し切り替えます。

[Timestamps for log file entries]

デバッグログメッセージに付与される時間情報を指定します。

・**[UTC] 選択**　：UTC(国際協定時刻;Coordinated Universal Time)(グリニッジ標準時; GMT と同義) で表示。

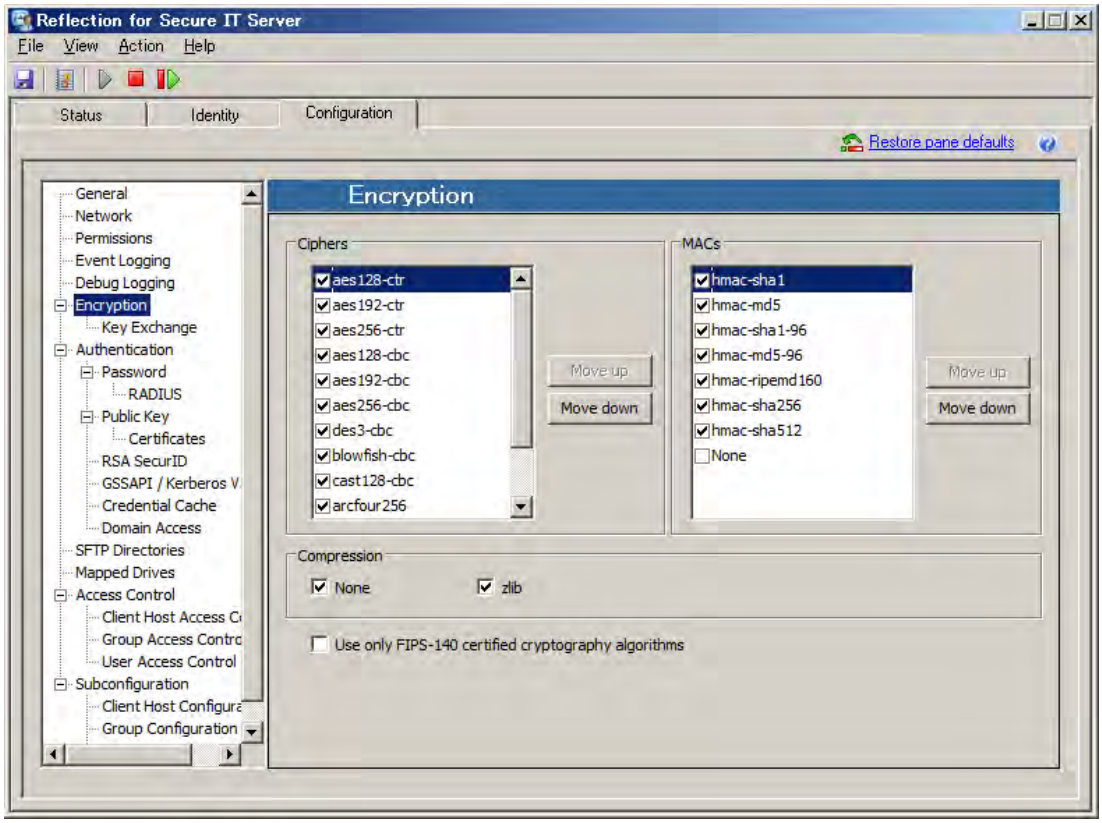
・**[Local] 選択**：指定タイムゾーン時刻で表示。

[View latest log file] ボタン　　*…〈7.2 SP1 から追加〉*

最新(現行)のデバッグログ内容を表示します。

尚、メニューからの選択 "View" > "Latest Debug log File" でも同様に表示します。

4.2.6 [Encryption] 設定画面



[Ciphers]

送受信するデータやパスワード等の情報を暗号化する共通鍵の暗号方式を指定します。

表中上位のものが、クライアントとの接続開始ネゴシエーション時に候補として優先使用されます。チェックマークの on/off と up/down により指定します。

{aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192- cbc, aes256- cbc, des3-cbc, blowfish-cbc, cast128-cbc, arcfour256, arcfour128, arcfour, none}をサポートしています。

注記：

"none"は、暗号化せずに平文のまま送信しますのでテスト解析用以外には禁止です。

[MACs]

データの完全性確認(=改ざんを検出)する MAC(Message Authentication Code)アルゴリズムを指定します。表中上位のものが、クライアントとの接続開始ネゴシエーション時に候補として優先使用されます。チェックマークの on/off と up/down により指定します。

{hmac-sha1, hmac-md5, hmac-sha1-96, hmac-md5-96, hmac-ripemd160, hmac-sha256, hmac-sha512, none}をサポートしています。

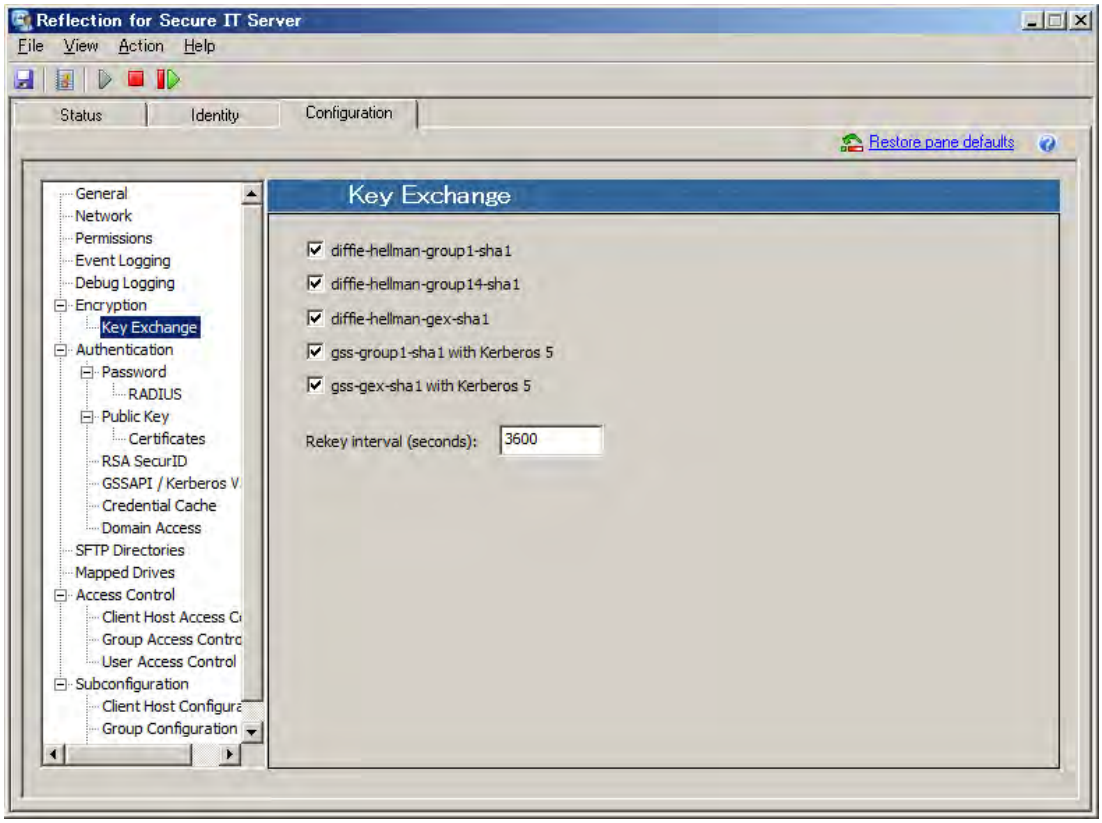
[Compression]

圧縮の指定です。

[Use only FIPS-140 certified cryptography algorithms]

FIPS 140-2 (米連邦政府情報処理規格 140-2) 認定の暗号モジュールのみを使用するように指定します。デフォルトは未チェック状態で、このまま使用することを推奨します。

4.2.7 [Key Exchange] 設定画面



送受信データ暗号化用セッション鍵を生成するための鍵交換アルゴリズムを指定します。

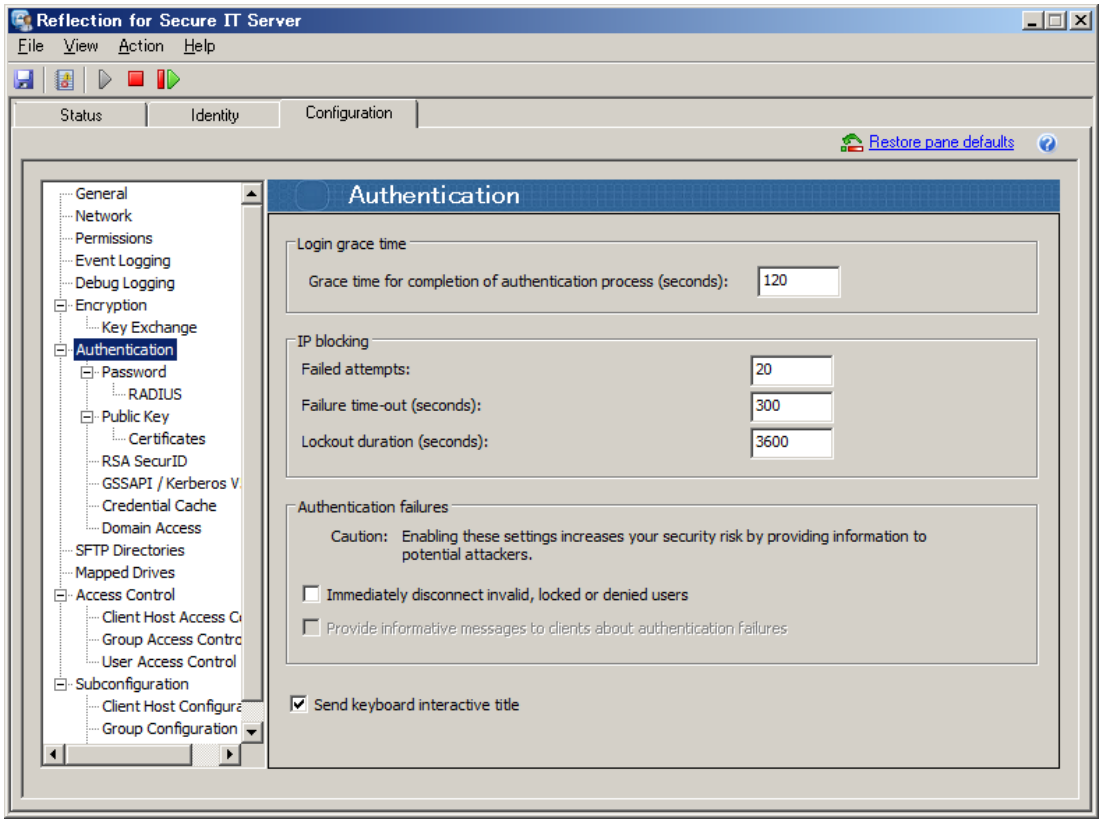
7.2 SP1 では、以下の鍵交換アルゴリズムに対応し、デフォルトでは全て候補としています。

{diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-gex-sha1,
gss-group1-sha1 with Keroberos 5, gss-gex-sha1 with Keroberos 5}

[Rekey interval (seconds):]

長時間 SSH 接続が継続している場合に、暗号化用セッション鍵を再生成 (= Rekey) する時間間隔を指定します。デフォルトは 3600(秒)です。

4.2.8 [Authentication] 設定画面



ユーザ認証に関して全体に共通する項目を指定します。

Login grace time

[Grace time for completion of authentication process (seconds):]

クライアント接続要求開始からユーザ認証成功までの最大許容待ち時間を秒単位で指定します。デフォルトは 120(秒)です。(バージョン 6.1 の時には デフォルト 600 秒でした。バージョンアップ時に旧バージョンの設定値を移行した場合はその値となっています。)

注記：

値"0" は無制限を意味しますが、保持状態継続によるシステムリソースの浪費や DoS 攻撃への配慮から、値"0" 指定は禁止とします。

IP blocking

ある特定の IP アドレスのクライアントから短時間に多くの接続失敗が繰り返された時に、その IP アドレスのクライアントに対し接続試行を一定時間ブロックすることが出来ます。

[Failed attempts:]に接続失敗回数上限値を指定し、[Failure time-out (seconds):]に基準となる監視時間を指定し、[Lockout duration (seconds):]にブロックし続ける時間を指定します。

[Failed attempts:]

IP ブロッキングする失敗回数を指定します。

デフォルトは 20(回)です。値"0" は IP ブロッキング機能の無効化を意味します

[Failure time-out (seconds):]

基準となる監視時間を指定します。

デフォルトは 300(秒)です。

[Lockout duration (seconds):]

IP ブロッキングの規定値になった時点からブロックし続ける時間を指定します。

デフォルトは 3600(秒)です。

注記:

IP ブロッキング機能は、パスワード認証とキーボードインターラクティブ形式によるパスワード認証による接続試行失敗の時にのみ機能します。

IP ブロッキングに関する管理情報をメモリ上に持つため、sshd サービスを再開した場合はそれまでの情報は無効になります。

Authentication failures

[Immediately disconnect invalid, locked or denied users]

"存在しない"、"ロックされている"、"拒否設定されている"といった認証が失敗することが自明なユーザに対しての接続要求があった場合に、初回で直ぐに接続失敗とし切断する動作を指定します。

デフォルトは非チェックで、接続要求ユーザに対し試行許容回数分の認証操作を求めます。

不正なアクセス者に対しては、デフォルトの非チェック状態の方がサーバ内のユーザに関する情報を遮蔽することになりますので、より安全と言えます。

[Provide informative messages to clients for authentication failures]

上記設定にチェックマークを入れ、初回で直ぐに接続失敗とし切断する場合に、その理由をクライアントに伝えるかどうかを指定します。セキュリティ上、決して推奨出来ません。

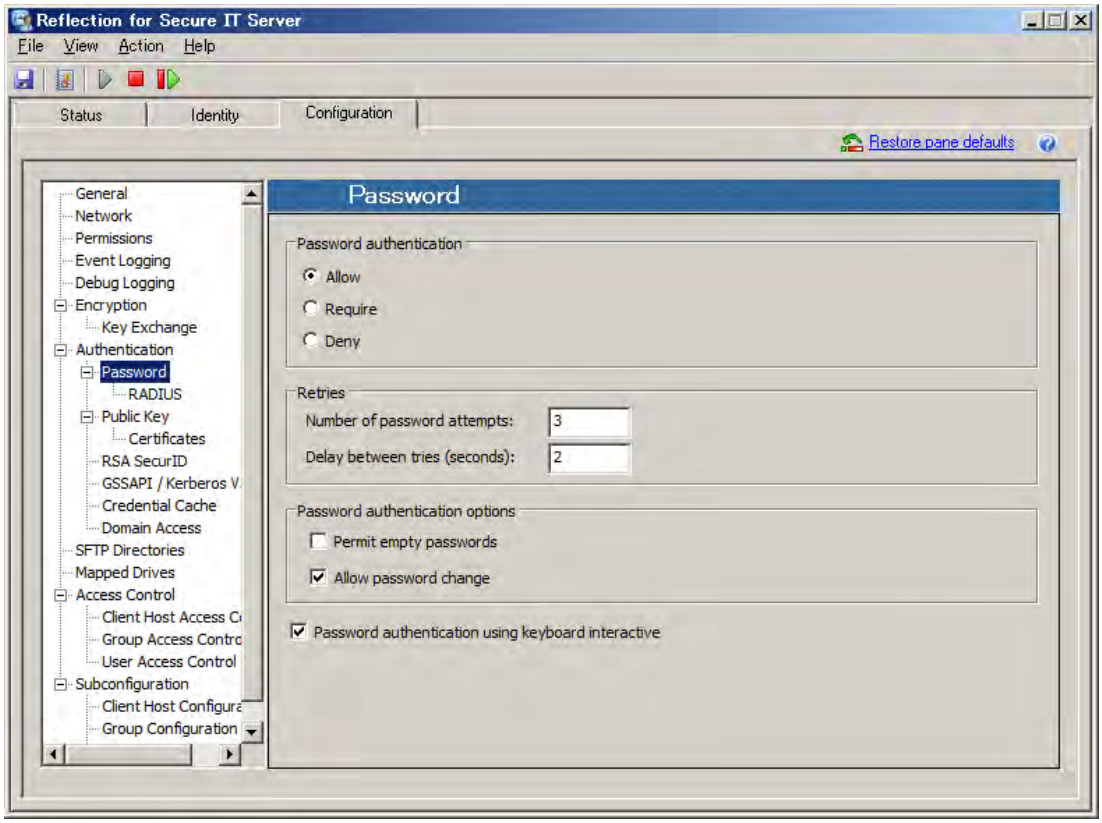
Keyboard interactive

[Send keyboard interactive title:]

キーボードインターラクティブ認証時にクライアント側画面上にタイトルテキストを表示するかどうかを指定します。

デフォルトはチェック付きで、従来通りタイトルテキストを表示します。

4.2.9 ［Password］設定画面



本設定画面を通じて、"パスワード認証"およびパスワード入力の"キーボードインターラクティブ認証"について指定します。

注記：

画面最下部［Password authentication using keyboard interactive］のチェックマーク有無が、**# Password authentication** 欄の｛Allow、Require、Deny｝の対象に影響します。

"Allow" と "Require" の意味について：

・"Allow" ～クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補対象として指定されます。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

・"Require" ～SSH サーバがクライアントに対してユーザ認証成功のために認証成功必須を要求する対象として指定されます。ユーザ認証成功のためには、"Require"として要求された認証方式全てが成功する必要があります。

Password authentication

(説明では、[Password authentication using keyboard interactive]を[KB int]と省略します。)

[Allow] 選択の場合:

[KB int] 選択時：パスワード認証、キーボードインターラクティブ認証両方に対して "Allow"

[KB int] 非選択時：パスワード認証に対して "Allow"

[Require] 選択の場合:

[KB int] 選択時：キーボードインターラクティブ認証に対して "Require"

[KB int] 非選択時：パスワード認証に対して "Require"

[Deny] 選択の場合:

[KB int] の選択にかかわらず、パスワード認証、キーボードインターラクティブ認証いずれもユーザ認証として使用せず。

Retries

[Number of password attempts]

一回の接続要求に対してユーザ認証失敗と見なす試行回数を指定します。

デフォルトの回数は 3 回です。

[Delay between tries (seconds)]

試行回数失敗後に再入力要求のプロンプトを表示する時間間隔を秒で指定します。

デフォルトの間隔は 2 秒です。

Password authentication options

[Permit empty passwords]

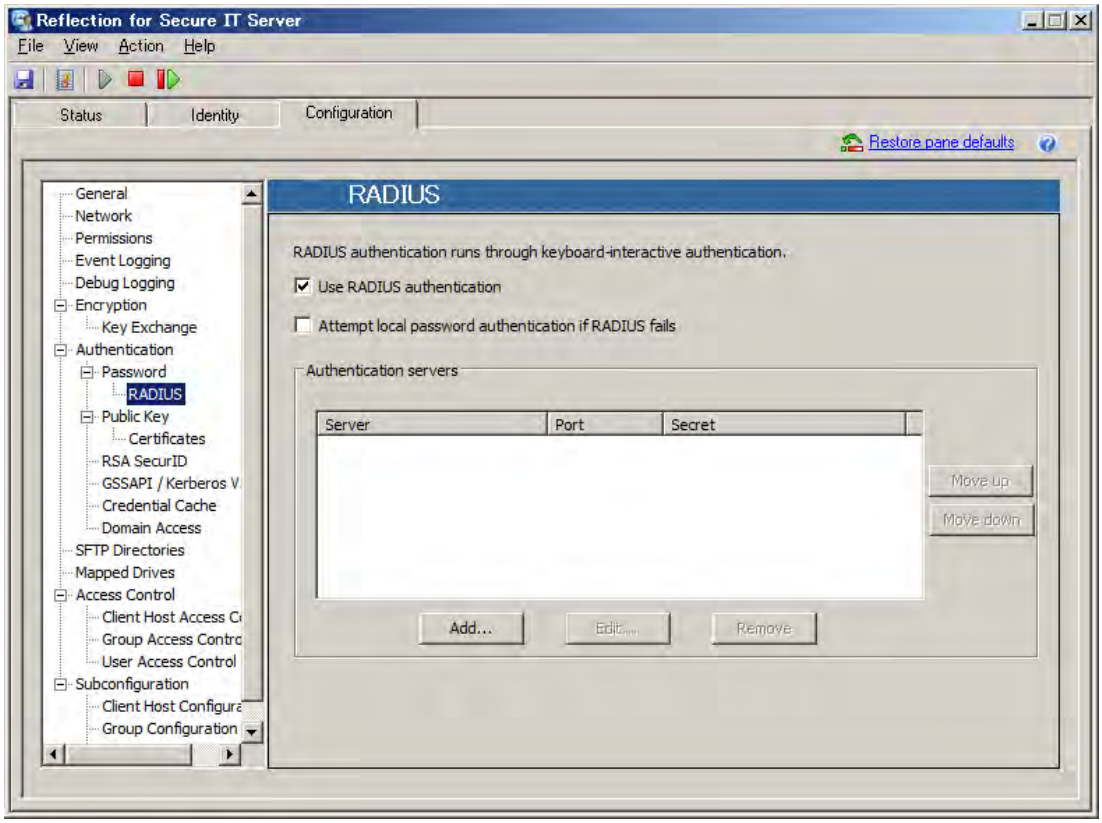
空(=空白)パスワードを許容する時、チェックを入れます。デフォルトは、禁止です。

最終的には、本設定以外に Windows OS の ポリシーの影響も受けます。

[Allow password change]

接続開始時のユーザ認証処理手順の中で OS 要求のパスワード変更処理を許すかどうかを指定します。

4.2.10 [RADIUS] 設定画面



RADIUS サーバとの連携によりユーザ認証を実現するための指定をします。

設定画面内一行目に英文で記述のように、RADIUS 認証は、キーボードインターラクティブ認証を通じて実行されます。

よって、[Password]設定画面において次の指定をした場合は、RADIUS 認証は使用出来ずに、[RADIUS]設定画面自体がグレーアウトします。

①[Password authentication]で"Deny"を選択

②[Password authentication using keyboard interactive]を非選択

注記：

ログインユーザが、サーバローカルか Windows ドメインユーザとして存在しない場合は、RADIUS サーバで認証可能でも、SSH の認証自体は失敗します。

[Use RADIUS authentication]

RADIUS サーバとの連携によるユーザ認証を有効化します。

[Password]設定画面において、①[Password authentication]で"Deny"を選択、②[Password authentication using keyboard interactive]が非選択 の時には、無効化しています。

[Attempt local password authentication if RADIUS fails.]

RADIUS サーバとの連携によりユーザ認証が失敗した時に、サーバローカルのパスワードを使用してユーザ認証をするか指定します。

Authentication servers

RADIUS Server ダイアログボックス

[Server]

RADIUS サーバの名称または IP アドレスを設定します。

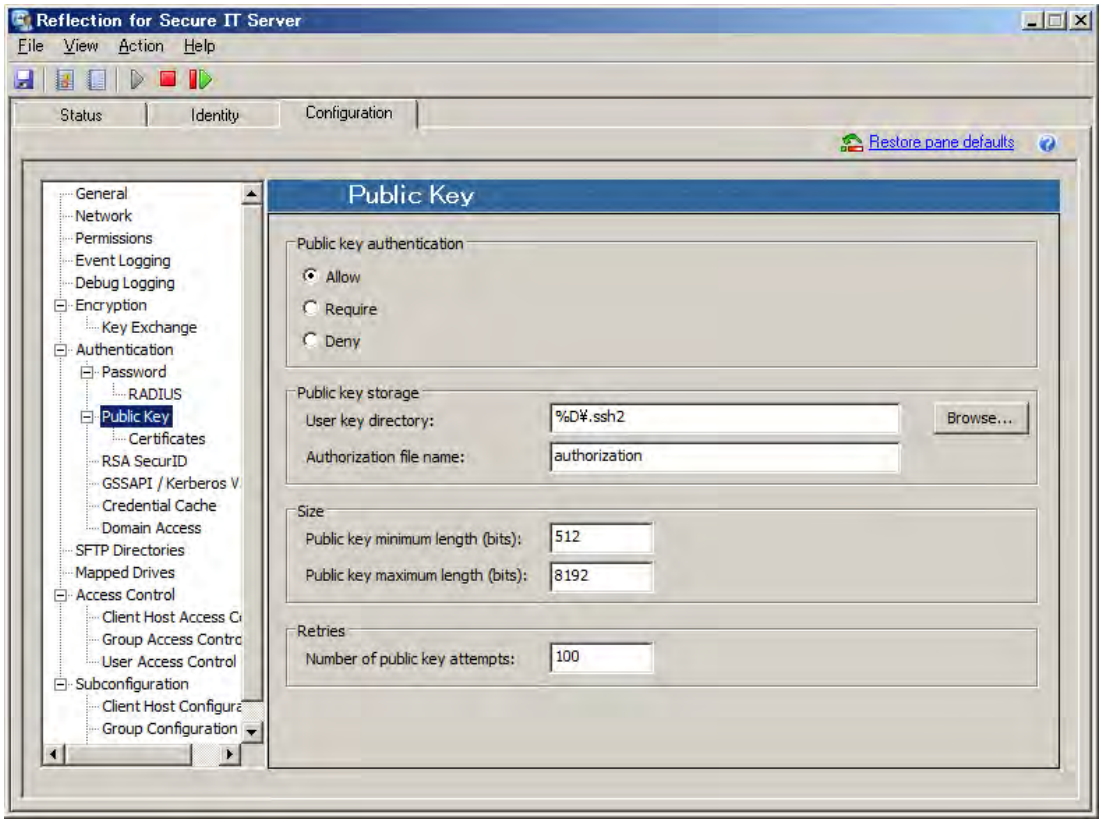
[Port]

使用するポート番号を指定します。

[Secret]

RADIUS サーバとの接続のために、RADIUS に対するホストのパスワードを設定します。

4.2.11 ［Public Key］設定画面



公開鍵認証によるユーザ認証を実現するためのサーバ側設定をします。

Public key authentication

[Allow] 選択：

クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補として公開鍵認証を指定します。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

[Require] 選択：

SSH サーバがクライアントに対してユーザ認証として公開鍵認証を要求します。ユーザ認証成功のためには、"Require"として要求された全て認証方式に成功する必要があります。

[Deny] 選択：

ユーザ認証として公開鍵認証を使用しない指定です。

Public key storage

[User key directory:]

公開鍵認証で使用するユーザの登録公開鍵の所在ディレクトリを指定します。

パスで直接指定するか、パターンストリング("%D","%H","%u","%U")を使用可能です。

デフォルトは %D¥.ssh2 (Windows ユーザプロファイル下の".ssh2"フォルダ) です。

- %D：ユーザプロファイルフォルダ
- %H：ユーザホームフォルダ
- %u：ユーザログイン名
- %U：ドメインユーザログイン名 (domain.username の書式)

[Authorization file name:]

登録公開鍵ファイル名をリストアップした管理ファイル名を指定します。

デフォルト名称は "authorization"ファイルです。

Size

[Public key minimum length (bits):]

使用可能な公開鍵の最小のビット長を規定します。

範囲は 512～8192 で、デフォルト 512 (ビット長)です。

[Public key maximum length (bits):]

使用可能な公開鍵の最長のビット長を規定します。

範囲は 512～8192 で、デフォルト 8192 (ビット長)です。

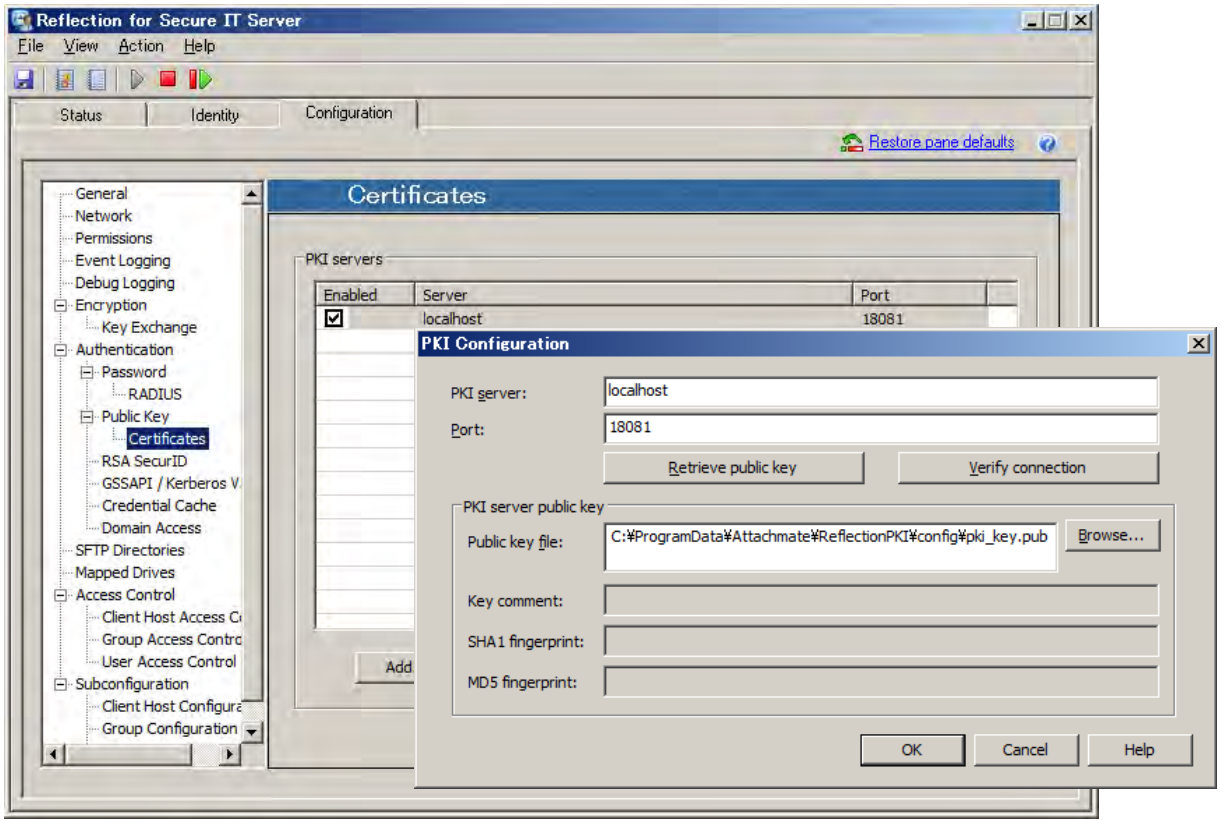
Retries

[Number of public key attempts:] *…〈7.2 SP1 から追加〉*

公開鍵認証を用いた接続確立処理において、クライアント内に秘密鍵が複数存在する場合は、クライアントは一つ目の秘密鍵からユーザ認証が成功するまで順次保管秘密鍵を使って認証試行を繰り返します。本設定は、サーバ側でその試行回数に制限を加えるために存在します。

デフォルトは 100 です。(…従来運用に影響ないように常識的には限りなく大きな値としました。)

4.2.12 [Certificates] 設定画面



ユーザ認証として証明書認証を使うための設定をします。

RSIT Windows サーバは、外部認証局と連携して証明書認証を実現するために、弊社別製品の「Reflection PKI Services Manager」(無償)を仲介して動作します。本設定では、その「Reflection PKI Services Manager」との通信のための指定をします。(「Reflection PKI Services Manager」の詳細については、英文マニュアルを参照して下さい。)

7.2 SP1 からは、高可用性 PKI 環境実現のために複数の「Reflection PKI Services Manager」と連携可能になりました。よって、複数対応可能な設定とするために、個々の[PKI Configuration]ダイアログボックス設定画面を通じて設定可能です。

 # PKI Servers

[Server:]

対応する"Reflection PKI Services Manager" を示します。

デフォルトで "localhost" (= RSIT Windows サーバと同一サーバ内) が指定済みです。

[Port:]

"Reflection PKI Services Manager" が待ち受けるポート番号を指定します。

デフォルトは 18081 番ポートです。

[Add]/ [Edit]/ [Remove]ボタン

[PKI Configuration]設定画面を"新規追加"/"編集"/"削除"する指示ボタンです。

[Launch PKI Services Manager] ボタン

同一サーバ内に"Reflection PKI Services Manager" が存在する時有効なボタンで、"Reflection PKI Services Manager" を起動します

[PKI configuration]ダイアログボックス

[PKI server:]

通信先"Reflection PKI Services Manager" 稼働サーバを指定します。

デフォルトは "localhost" で、別サーバ指定時は、そのホスト名か IP アドレスを指定します。

[Port:]

"Reflection PKI Services Manager" が待ち受けるポート番号を指定します。

[Retrieve public key] ボタン

"Reflection PKI Services Manager" 認証用の公開鍵の確認と保存のための操作ボタンです。

[Verify Connection] ボタン

"Reflection PKI Services Manager" との正常通信を確認する指示ボタンです。

PKI Server Public key

[Public key file:]

"Reflection PKI Services Manager" との通信の認証に公開鍵認証を使用します。

"Reflection PKI Services Manager" をインストールすることで所定のディレクトリに鍵ペアが作成されます。RSIT Windows サーバを別マシンとする時に、この"Reflection PKI Services Manager" インストール時の公開鍵を、RSIT Windows サーバ側にコピーし、そのディレクトリを本設定にて指定します。

[Key comment:]

"Reflection PKI Services Manager" の公開鍵コピーした時に、その公開鍵のコメント内容を表示します。

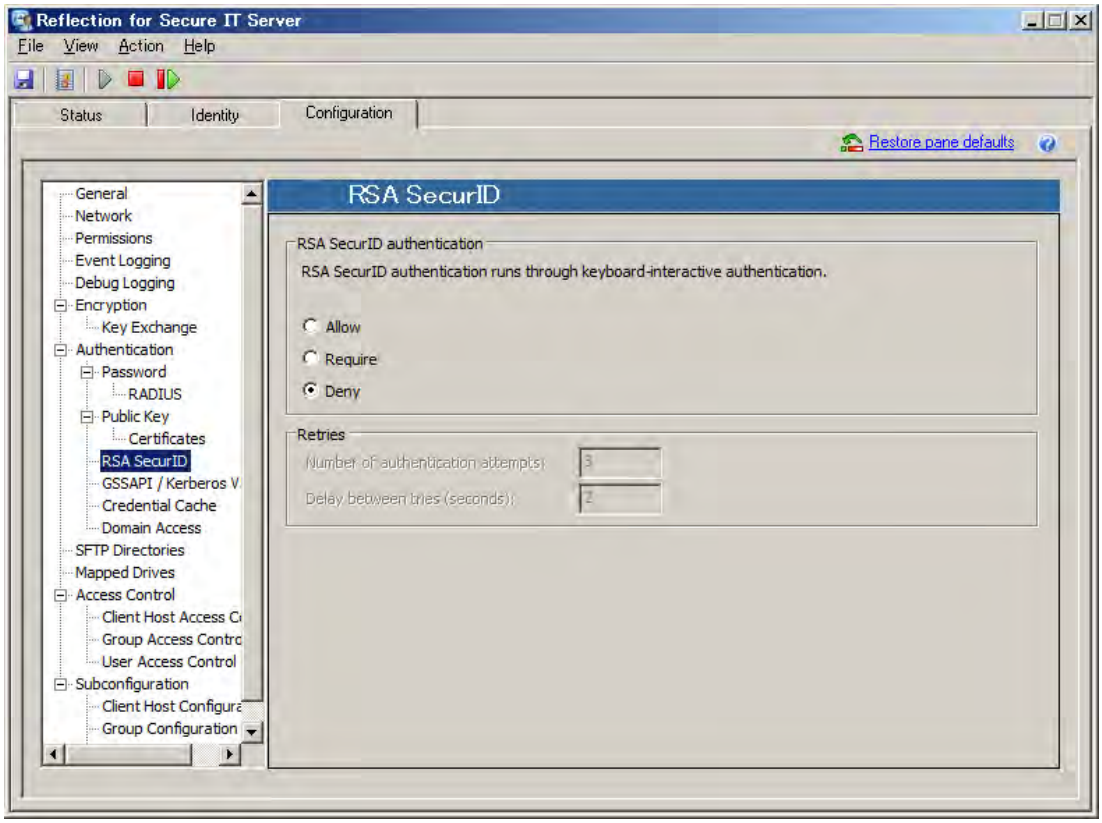
[SHA1 fingerprint:]

"Reflection PKI Services Manager" の公開鍵コピーした時に、SHA1 ハッシュ関数によるメッセージダイジェスト(=fingerprint) を表示します。

[MD5 fingerprint:]

"Reflection PKI Services Manager" の公開鍵コピーした時に、MD5 ハッシュ関数によるメッセージダイジェスト(=fingerprint) を表示します。

4.2.13 ［RSA SecurID］設定画面



RSA SecurID との連携によりユーザ認証を実現するための設定をします。

RSA SecurID を使用するために、RSA SecurID の環境設定が正しくされている必要があります。

特に RSIT Windows サーバを導入したサーバ内には、RSA Authentication Agent for Winodws か RSA Authentication Manager 自体を正しく実装します。

設定画面内上部に記述のように、RSA SecurID を利用したユーザ認証は、キーボードインターラクティブ認証を通じて実行されます。よって、[Password]設定画面において、①[Password authentication]を"Deny"選択か、②[Password authentication using keyboard interactive]を非選択の場合は、RSA SecurID 認証は使用出来ません。

注記：

ログインユーザが、サーバローカルか Windows ドメインユーザとして存在しない場合は、認証は失敗します。

RSA SecurID authentication

{Allow、Require、Deny} から選択します。デフォルトは "Deny"です。

[Allow] 選択：

クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補として指定します。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

[Require] 選択：

SSH サーバがクライアントに対してユーザ認証として要求します。ユーザ認証成功のためには、"Require" として要求された全て認証方式に成功する必要があります。

[Deny] 選択：

ユーザ認証として RSA SecurID 認証を使用しない指定です。

Retries

[Number of password attempts]

一回の接続要求に対してユーザ認証失敗と見なす試行回数を指定します。

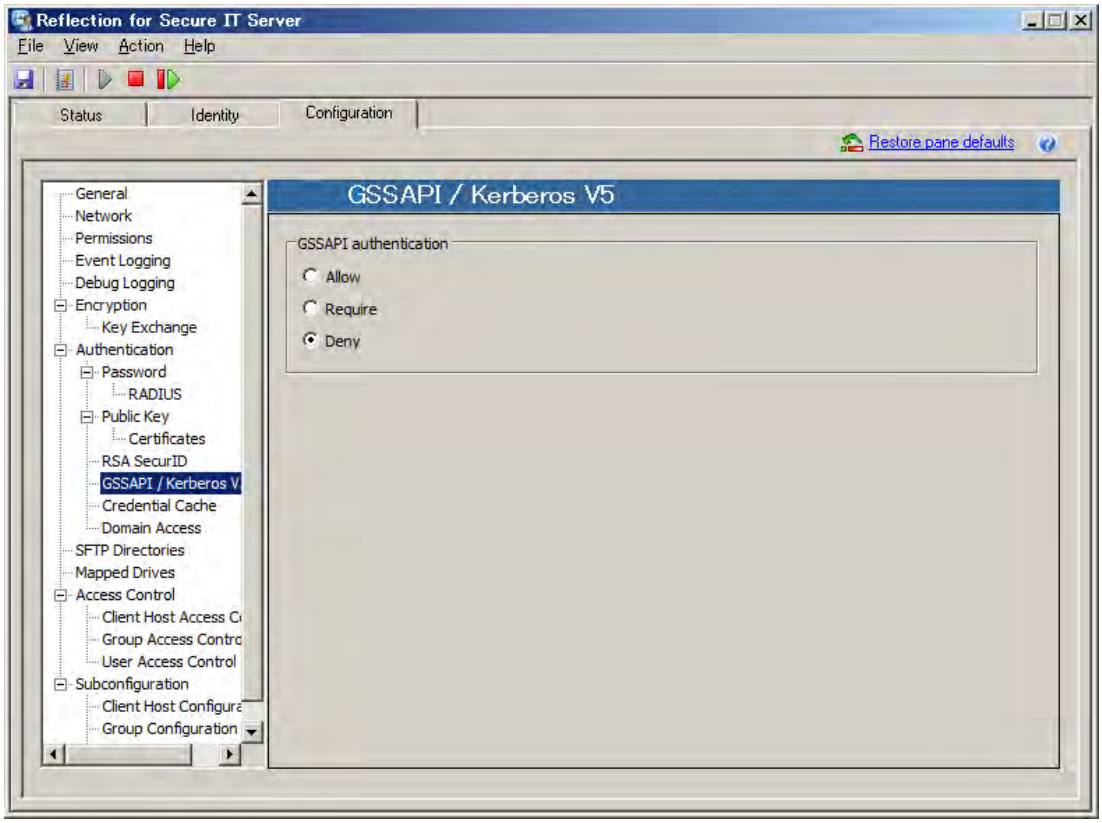
デフォルトの回数は 3 回です。

[Delay between tries (seconds)]

失敗後に再入力要求のプロンプトを表示する時間間隔を秒で指定します。

デフォルトの間隔は 2 秒です。

4.2.14 [GSSAPI/Kerberos V5] 設定画面



GSSAPI(Generic Security Service API) を用いた Kerberos V5 をユーザ認証として使用するかを指定します。

{Allow、Require、Deny} から選択します。デフォルトは "Deny"です。

[Allow] 選択：

クライアントとのネゴシエーション時に SSH サーバが提示する使用認証方式の候補として指定します。最終的には、ネゴシエーションで決定された認証方式のうちのいずれかが認証成功すればユーザ認証が成功となります。

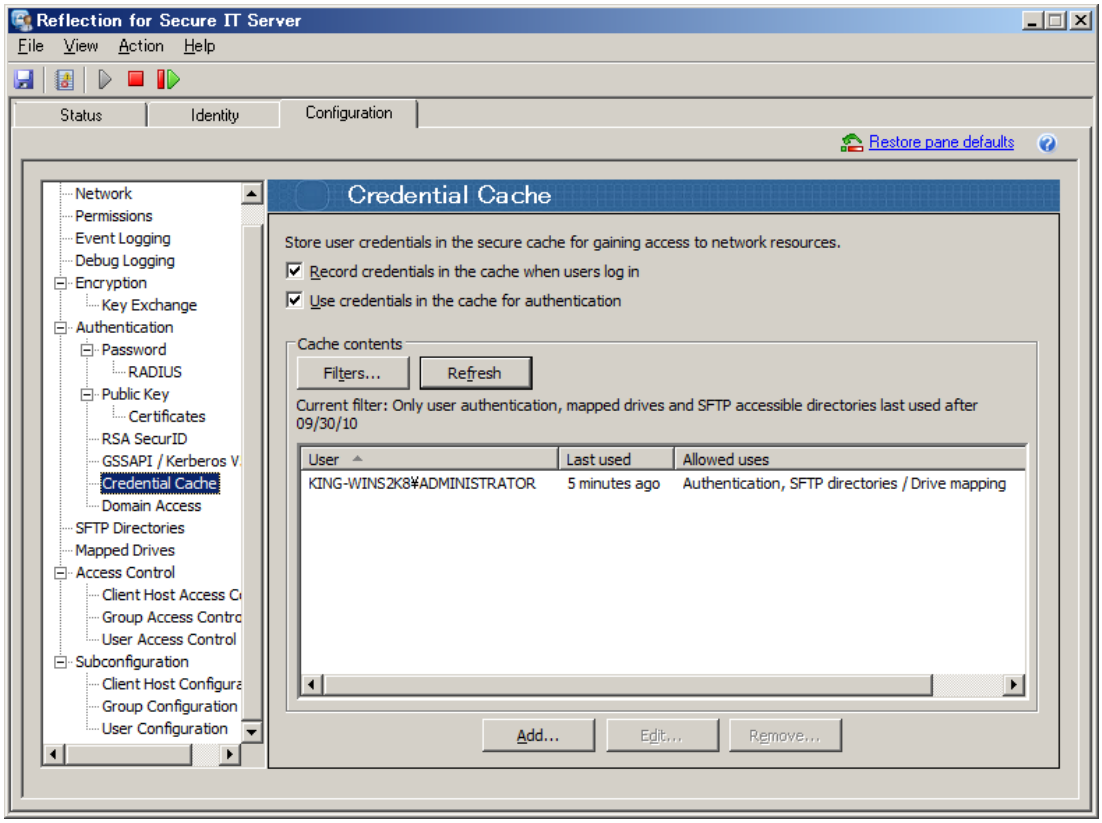
[Require] 選択：

SSH サーバがクライアントに対してユーザ認証として要求します。ユーザ認証成功のためには、"Require" として要求された全て認証方式に成功する必要があります。

[Deny] 選択：

ユーザ認証として Kerberos V5 認証を使用しない指定です。

4.2.15 [Credential Cashe] 設定画面



クライアントから接続する際に SSH サーバの先のネットワークリソースにアクセスするケースにおいて、ネットワークリソースへのアクセス認証に クライアントのユーザ認証情報以外の認証情報を使う場合に、本設定画面を使い指定します。定義情報は、暗号化し保存されます。

〈ネットワークリソースへのアクセスに認証情報が必要な例〉

(1)Windows ドメインユーザ認証確認時に、クライアントからのユーザ認証でパスワード情報入力が伴わない 公開鍵認証、証明書認証、SecurID 認証の場合

(2)[SFTP Directories]設定画面 "SFTP accessible directories" にネットワーク上のディレクトリを定義し、そこへのアクセスにクライアントのユーザ認証情報以外の認証情報を使う場合

(3)[Mapped Drives]設定画面にて定義したネットワークドライブへのアクセス認証として、クライアントのユーザ認証情報以外の認証情報を使う場合

[Record credentials in the cache when users log in]

選択有効時に、ネットワークリソースアクセスに必要なパスワード入力をユーザに要求し、入力された場合にそれを保存登録します。

[Use credentials in the cache for authentication]

選択有効時に、登録保存された有効なユーザ認証情報がある場合に外部ネットワークリソースへの認証に使用します。

Cache contents

[Filters] ボタン

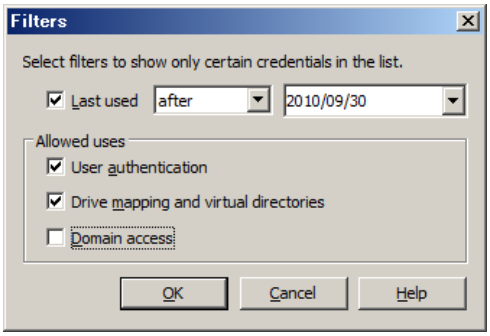
[Filters]ダイアログボックスを表示する指示ボタンです。

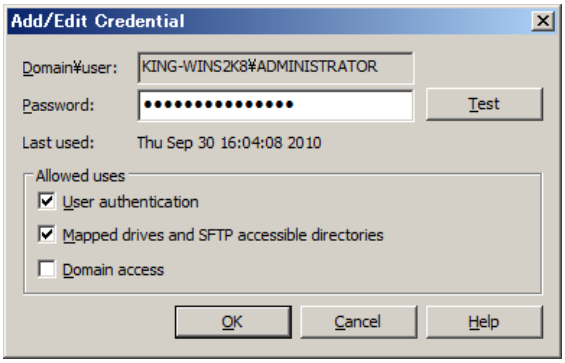
[Refresh] ボタン

Cache contents 欄の内容を更新するボタンです。

[Current filter]

[Filters]ダイアログボックス上で設定された条件内容を文章で表示します。





 # [Filters]ダイアログボックス：

登録保存されたユーザ認証情報の使用条件/表示条件を指定します。

[Last used]

Cache contents 欄に表示するユーザ認証情報の表示条件を指定します。

 # Allowed users

[Authentication],[Drive mapping and vitual directories],[Domain accessLast used]選択

選択有効化した項目に対して、登録保存されたユーザ認証情報を使用可能とします。

 # [Add/Edit Credential]ダイアログボックス：

ユーザ認証情報を登録する指定画面です。

[Domain¥user:]

定義するユーザ情報を Domain¥user 又は Computer 名¥user の形式で指定します。

[Password:]

定義するユーザ認証情報を指定します。

[Test]ボタン

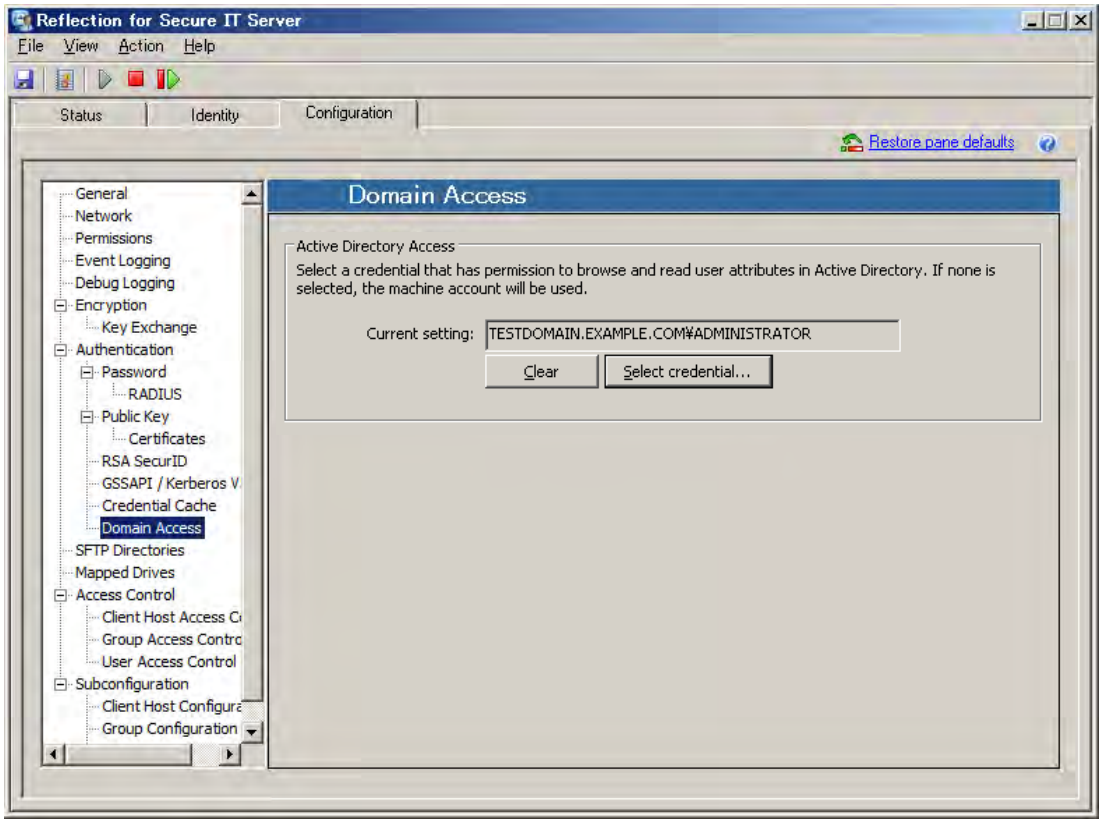
クリックすることで、指定ユーザ認証情報を使い実行します。

 # Allowed users

[Authentication],[Drive mapping and vitual directories],[Domain access]選択

選択有効化した項目に対して、登録保存されたユーザ認証情報を使用可能とします。

4.2.16 [Domain Access] 設定画面



RSIT Windows サーバを導入したサーバが Active Directory ドメインコントローラに対して確認要求する際のアクセス情報(credential)を設定します。

ドメインユーザでログインし、かつ下記条件のいずれかの場合に設定する必要があります。

1) ユーザ認証として、公開鍵認証、証明書認証、RSA SecurID 認証、RADIUS 認証のいずれかを使用し、かつ [Credential Cashe] 設定を通じてパスワードキャッシュを使用しない場合
2) RSIT Windows サーバの[Access Control]設定にて、Active Directory グループメンバシップの情報を使用している場合
3) RSIT Windows サーバの[Group Configuration]設定にて、Active Directory グループメンバシップの情報を使用している場合

また設定要否は、Active Directory ドメインコントローラの設定内容にも依存します。もし本設定が未設定で、かつパスワード情報を伴わない場合、RSIT Windows サーバは Local System アカウントを使いアクセスします。Active Directory ドメインコントローラ側で、本サーバの Local System アカウントにドメインユーザ属性情報リード権限を付与せず、更に匿名ユーザに許可を与えない設定をしていれば、Active Directory ドメインコントローラを使い認証判定は出来ずユーザ認証は失敗します。

[Current setting]

設定された Active Directory ドメインコントローラへのアクセスアカウントを表示します。

未設定の場合、Local System アカウントが使用されます。

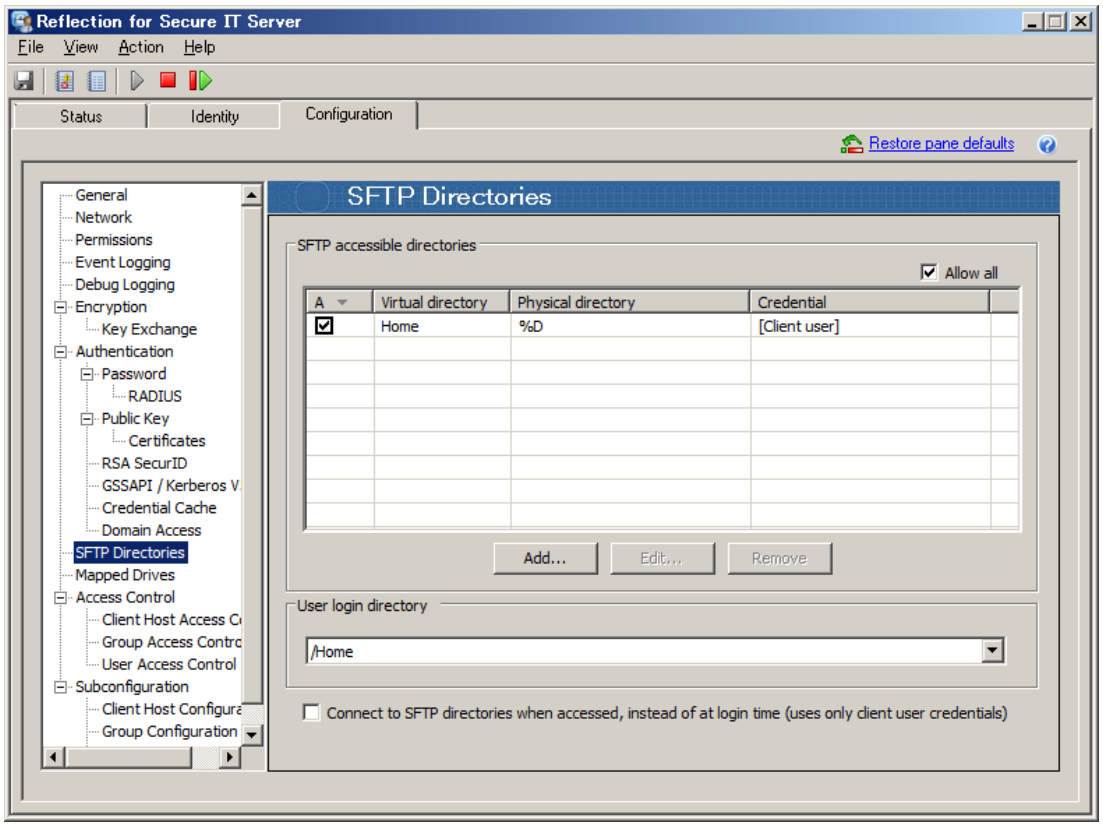
[Clear]ボタン

現設定内容をクリアします。

[Select credential]ボタン

[Select Credential]ダイアログボックスを開きます。その中で、既存ユーザ Credential キャッシュの中から選択指定したり、新規ユーザを選択指定します。

4.2.17 ［SFTP Directories］設定画面



本設定画面において、クライアントからの SFTP および scp アクセスにおけるアクセスユーザに対する ①アクセス許可範囲の指定、②ログインディレクトリの指定 をします。

［SFTP Accessible directories］

ユーザアクセス許可範囲をその最上位ディレクトリを記述して指定します。

複数列挙可能です。登録後に、チェックマークにて個別に有効/無効の指定も可能です。

［User login directory］

ログインディレクトリを指定します。プルダウンメニューに表示された"Virtual directory"名称〔7.2 SP1 時〕あるいは"Physical directory"名称〔7.2 以前〕から選択し指定します。

デフォルトは、"/Home"〔7.2 SP1 時〕又は "%D"(Windows ユーザプロファイル)〔7.2 以前〕です。

↓(*)7.2 SP1 Update1 にて追加

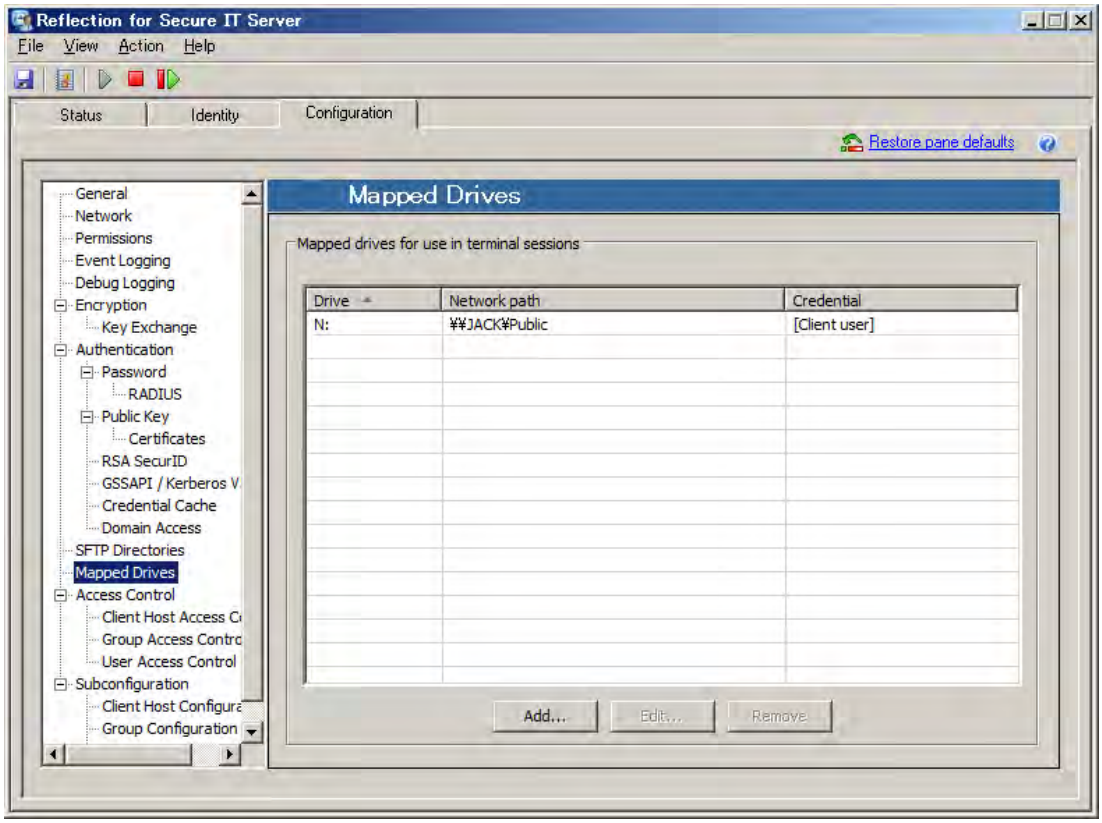
［Connect to SFTP directories when accessed, instead of at login time］

設定"SFTP accessible directories"先を内部接続するタイミングについて、ログイン時(デフォルト)の代わりに、実際に接続要求された時に接続実行する選択オプション

〈設定目的〉："SFTP accessible directories"を極端に多数設定した特別な使用環境において、ユーザのログイン処理時間を短縮改善するために設置。

通常使用ケースでは、デフォルトのまま使用することを強く推奨。

4.2.18 ［Mapped Drives］設定画面



本設定画面において、ネットワークドライブをマッピング定義し、ターミナル接続においてアクセス可能とします。

Mapped drives for use in terminal sessinons 欄

[Drive]

マッピングされたドライブ文字を表示します。

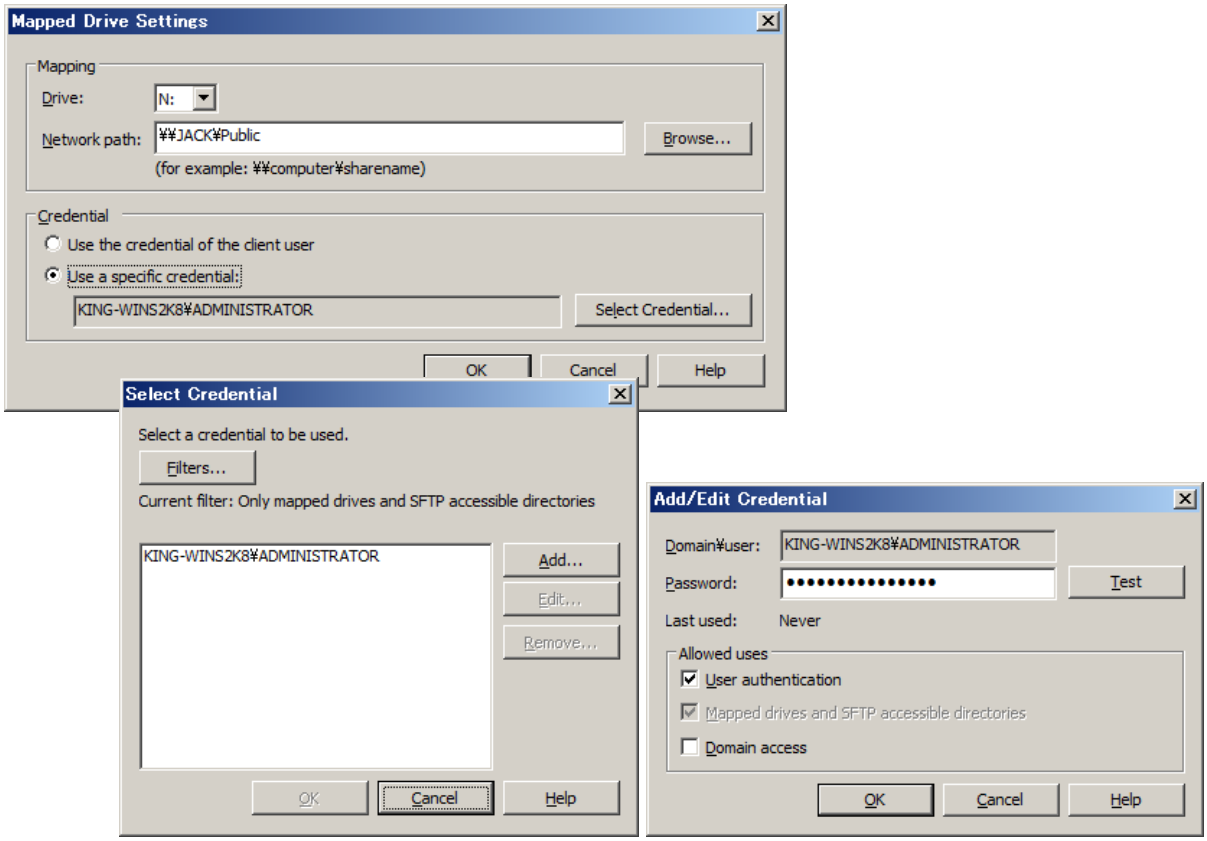
[Network path]

マッピングされたネットワークパスを UNC 形式で表示します。

[Credential]

登録した認証情報でアクセス権を得ているユーザ名を表示します。

[Client user]と表示している場合は、アクセスユーザが使用する認証情報を使います。



[Mapped Drives Settings]ダイアログボックス:

Mapping

[Drive:]

プルダウンメニューで表示する未割当のドライブ名から選択します。

[Network path:]

定義するネットワークパスを UNC 形式で指定します。〔例：¥¥computername¥path¥folder〕

直接入力するか、[Browse]ボタンクリックの上、[フォルダの参照]画面を操作して選択します。

Credential

[Use the credential of the client user]

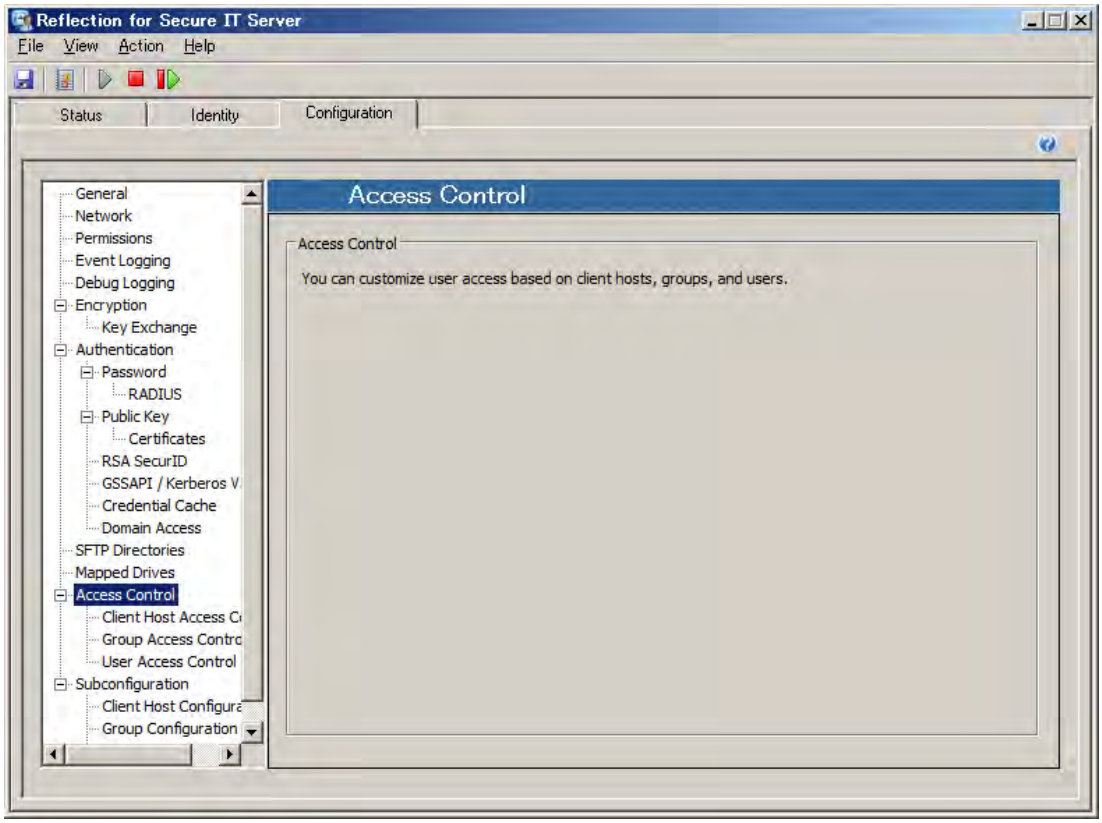
選択時(デフォルト)、クライアントユーザが持つユーザ認証情報を使いアクセス先ネットワークパスへのアクセス可否の認証を受けます。

[Use a specific credential:]

選択時、定義ネットワークパスへは、ここで定義するユーザアカウントとパスワードを使いアクセスします。[Select Credential]ボタンをクリックし、[Select Credential]設定画面を表示した上で、ユーザ認証情報を登録定義します。

[Select Credential]設定画面上の [Add],[Edit]ボタン操作にて、更に[Add/Edit Credential]設定画面を表示し、個々のユーザ認証情報を登録定義します。

4.2.19 [Access Control] 設定画面



[Access Control] 設定として、３つの観点からアクセス制御(許可/拒否指定)を指定可能です。

① [Client Host Access Control]：クライアント単位で指定

② [Group Access Control]：グループ単位で指定

③ [User Access Control]：ユーザ単位で指定

各設定とも、[Add]、[Edit] ボタンをクリックして、ダイアログボックスを表示し入力編集します。

入力文字は正規表現にて解釈されます。正規表現の場合、".(ドット)" がメタ文字、"¥(バックスラッシュ or 円マーク)" がエスケープコードとして扱われますので注意が必要です。

指定内容は次の規則に従い適用されます。

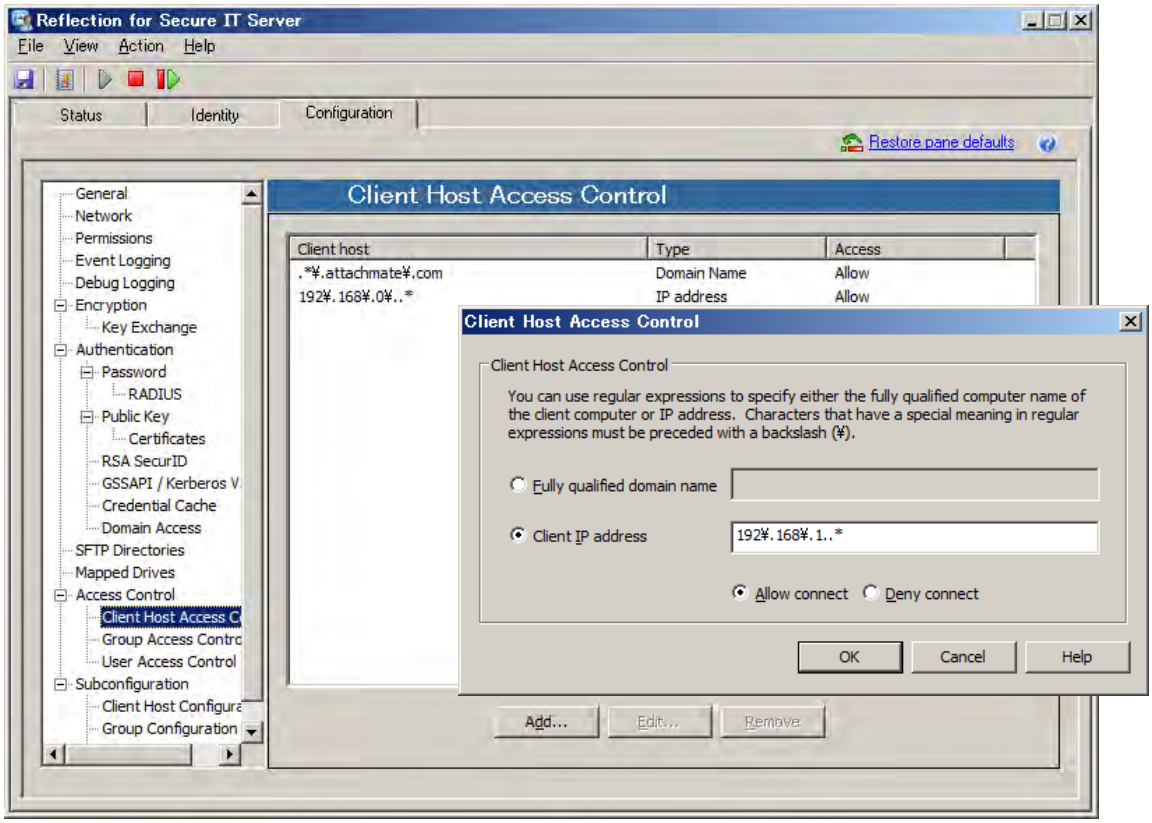
1) クライアント単位の"拒否"に該当する場合は、グループ単位/ユーザ単位の指定内容にかかわらずアクセスは拒否されます。

2) クライアント単位の"拒否"に該当しない場合、次にいずれかの設定画面に個別の"許可"指定が存在するかどうかを確認します。

2a) 個別の"許可"指定が全く存在しない場合は、アクセスは許可されます。

2b) いずれかの設定画面で個別の"許可"指定が存在する場合は、その"許可"指定条件に合致しない限り、アクセスは拒否されます。

4.2.20 [Client Host Access Control] 設定画面



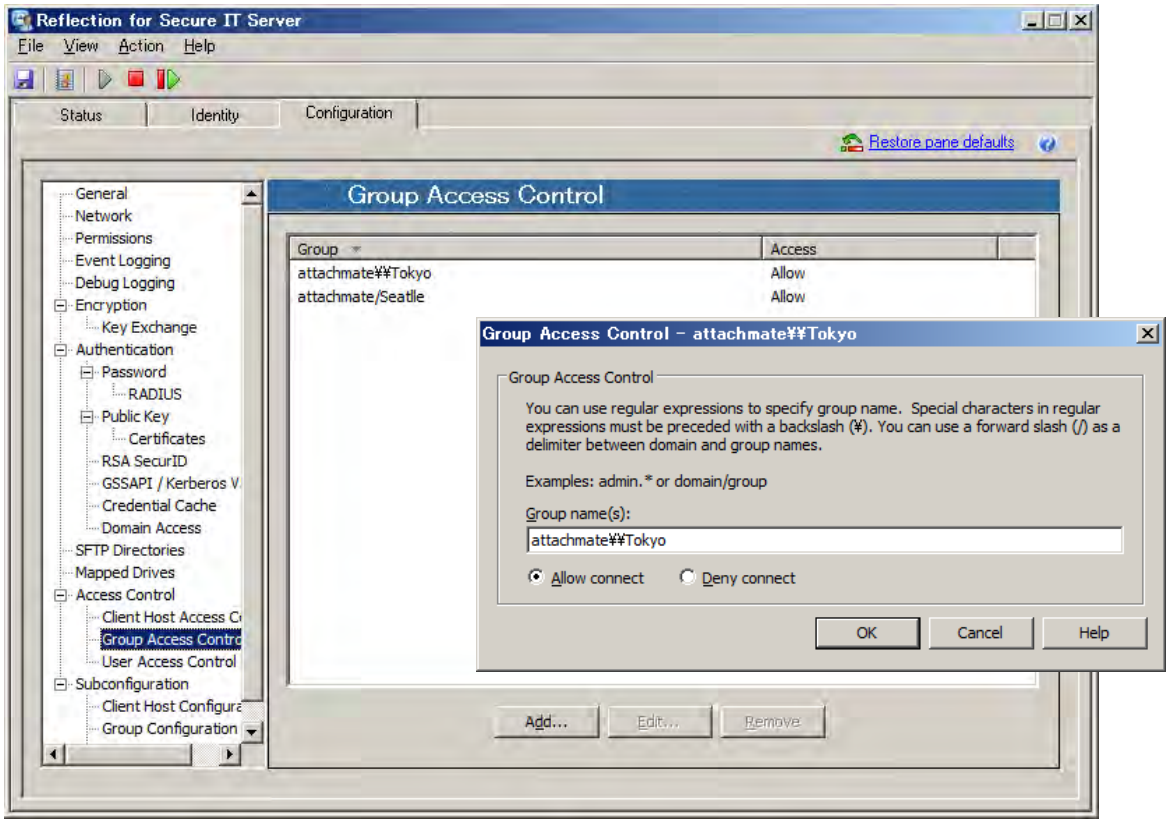
クライアント単位でのアクセス制御(許可/拒否指定)を指定します。

[Add]、[Edit] ボタンをクリックし、ダイアログボックスから入力編集します。

指定は、ドメイン名か IP アドレスにて指定します。

正規表現による解釈ですので、特に、ドメイン名や IP アドレスの区切りとしての ″.(ドット)″ の前にエスケープコード ″¥″ を付け、メタ文字 ″.(ドット)″ と識別する必要があります。

4.2.21 ［Group Access Control］設定画面



グループ名指定によりアクセス制御(許可/拒否指定)を指定します。

[Add]、[Edit] ボタンをクリックし、ダイアログボックスから入力編集します。

Windows Active Directory ドメインのグループ名指定の書式は、以下の通りです。

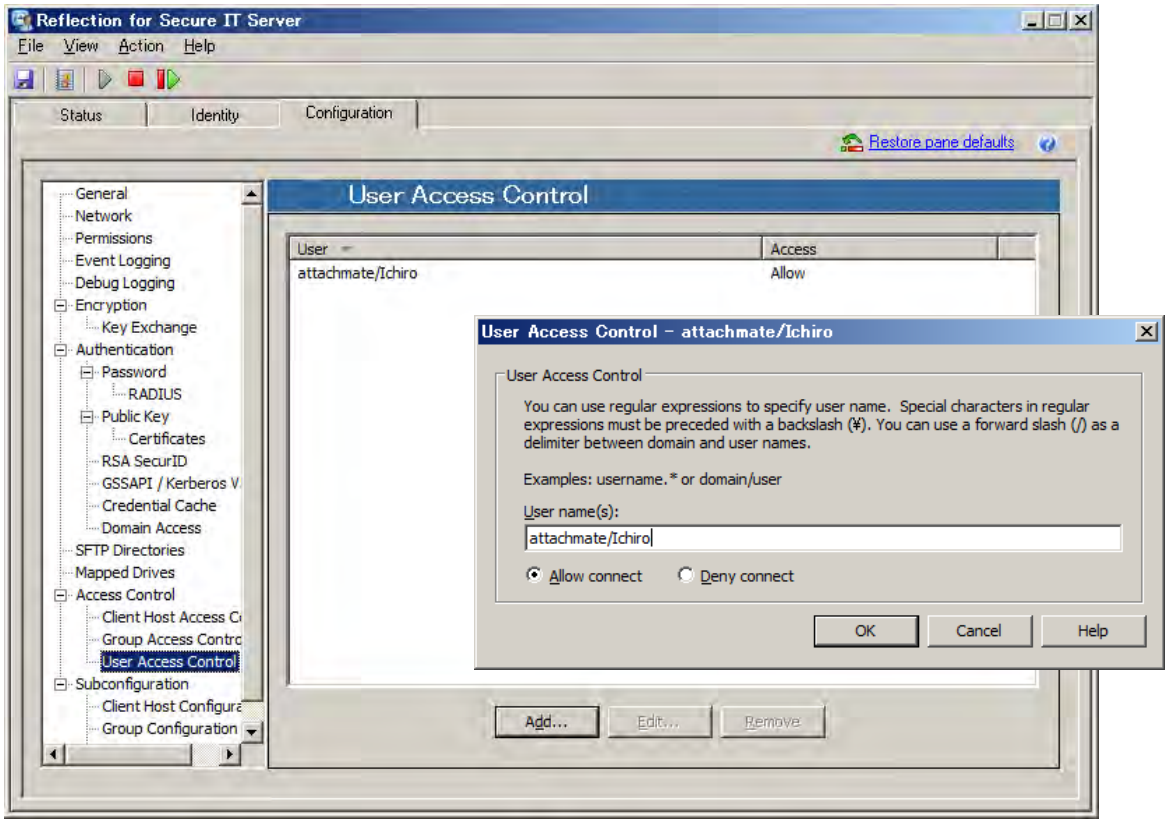
1) ①ドメイン名/グループ名 ②ドメイン名¥¥グループ名 のいずれも可能です。

2) グループ名にスペースを含む場合は、"[ ]"(大かっこ)で囲みます。

注記：

指定内容は正規表現により解釈します。よって、ドメイン名.グループ名 の書式でも一見動作する場合が多いのですが、メタ文字 ".(ドット)" と解釈され、改行を除く任意の一文字扱いになります。よって、".(ドット)"の位置を別な文字に置き換えた内容とも合致することになります。

4.2.22 ［User Access Control］設定画面



ユーザ名指定によりアクセス制御(許可/拒否指定)を指定します。

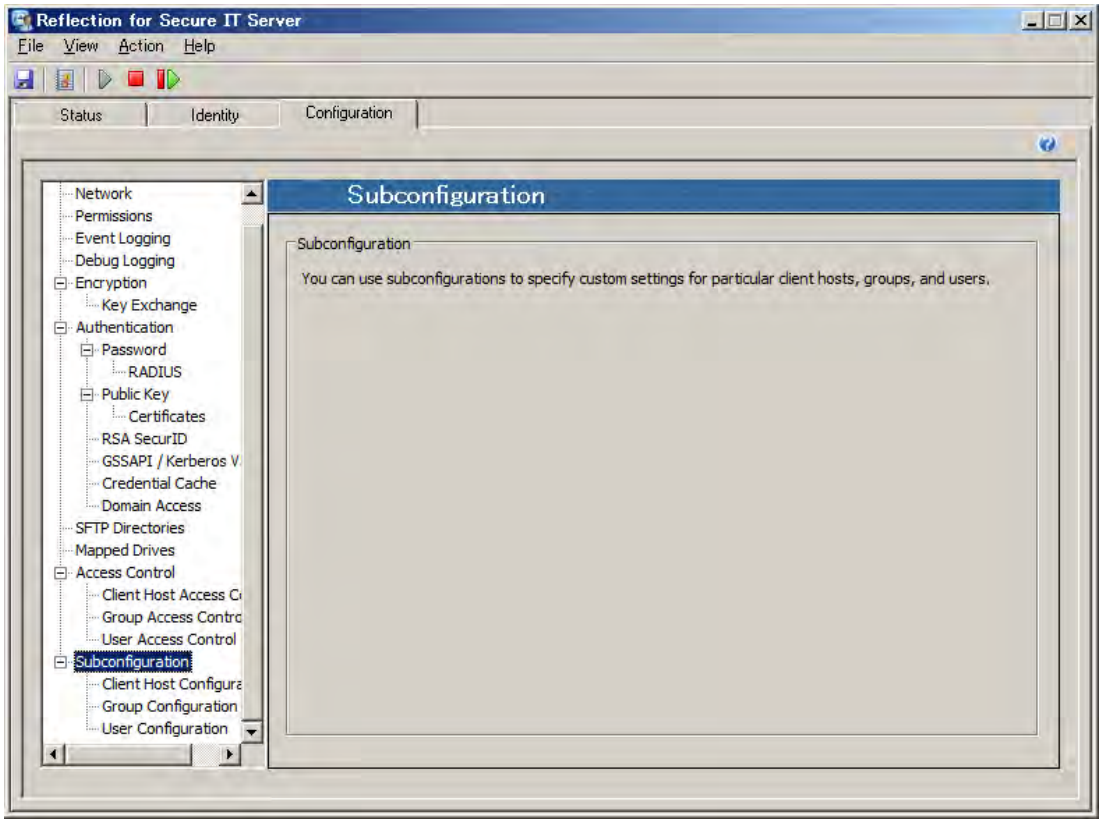
[Add]、[Edit］ボタンをクリックし、ダイアログボックスから入力編集します。

ドメインユーザ名指定の書式は、①ドメイン名/ユーザ名 ②ドメイン名¥¥ユーザ名　のいずれも可能です。

注記：

指定内容は正規表現により解釈します。よって、ドメイン名．ユーザ名 の書式でも一見動作する場合が多いのですが、メタ文字 ″.(ドット)″ と解釈され、改行を除く任意の一文字扱いになります。よって、″.(ドット)″の位置を別な文字に置き換えた内容も合致している状態になっています。

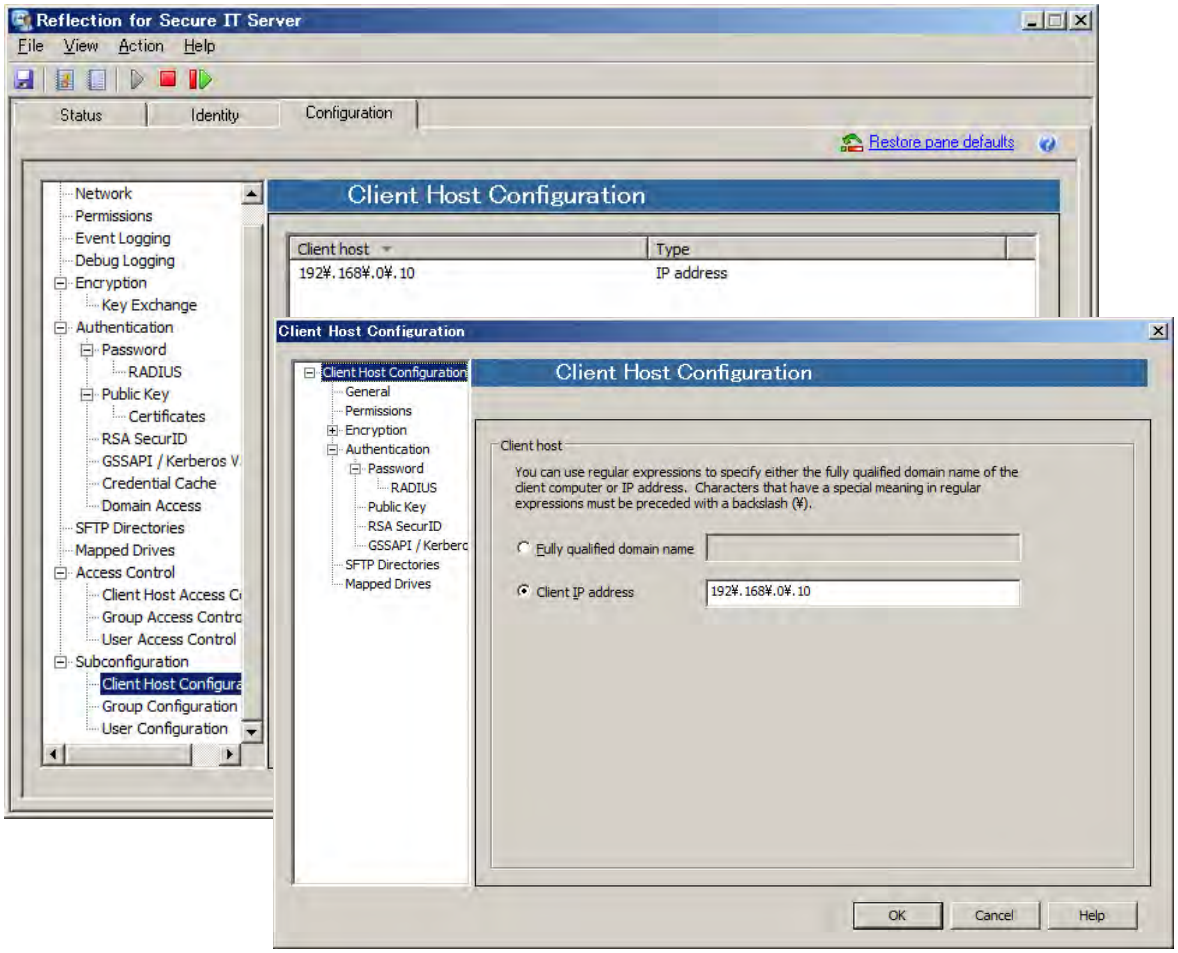
4.2.23 [Subconfigration] 設定画面



これまでの設定内容は導入したマシン共通に適用されます。これに対し、クライアント(Client Host Configuration) /グループ(Group Configuration) /ユーザ(User Configuration) 個別にサブコンフィギュレーション(Subconfiguration)を指定し、共通設定内容より高優先の指定が可能です。

RSIT Windows サーバは、次の順位で設定内容を読み込み、後から読み込んだ内容を上書きします。
①共通設定 ⇒ ② Client Host 個別設定 ⇒ ③ Group 個別設定 ⇒ ④ User 個別設定
よって最終的には、④>③>②>① の優先順位にて設定内容が適用されます。

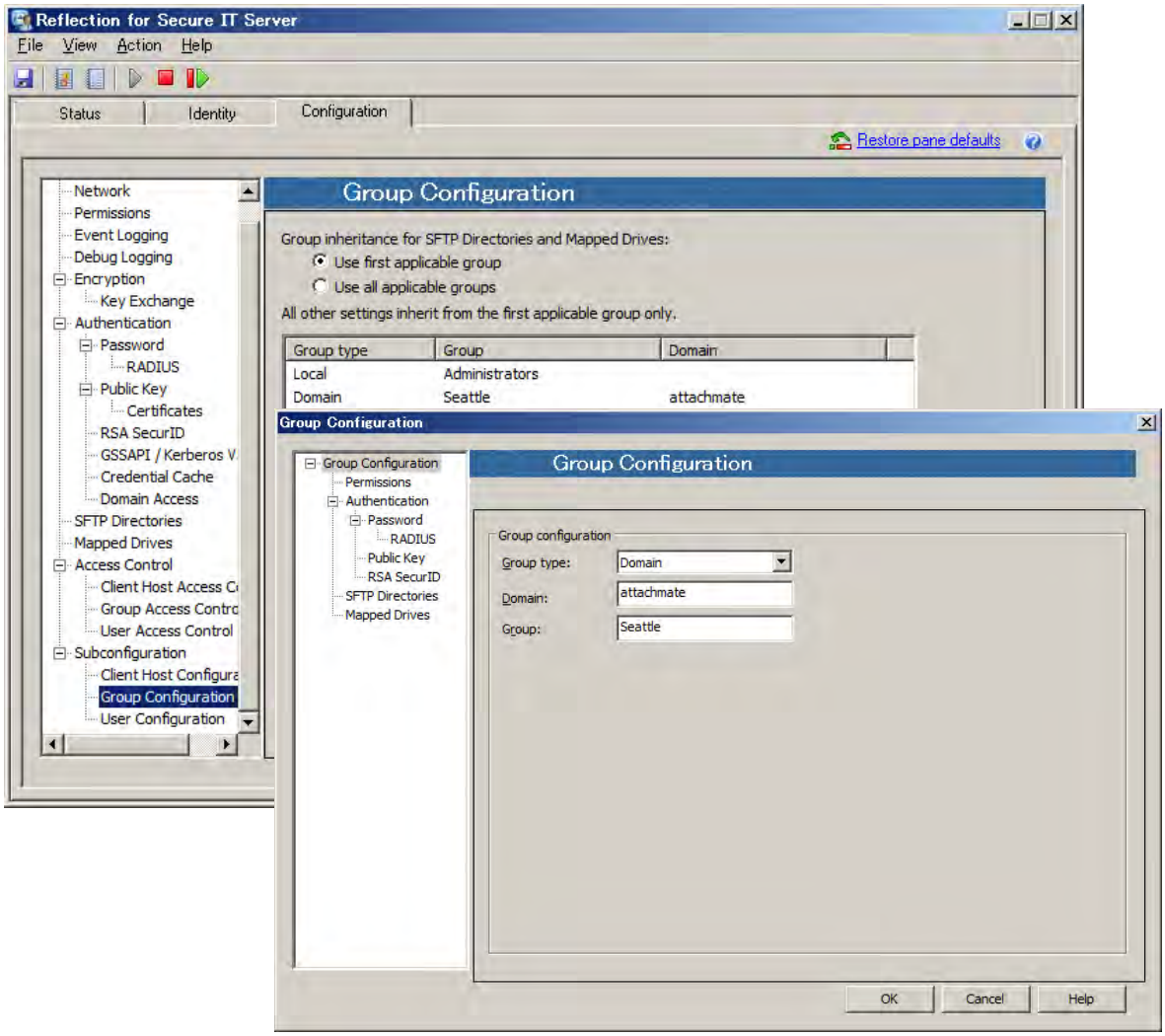
4.2.24 ［Client Host Configration］設定画面



設定画面内［Add］、［Edit］ボタンをクリックし、［Client Host Configuration］ダイアログボックスを表示し、指定クライアント(Client Host)に対して共通設定内容よりも高優先の個別指定をします。

クライアントとして ドメイン名か IP アドレスにて指定後に、左欄より設定内容を選択し、専用画面を通じて入力編集します。

4.2.25 [Group Configration] 設定画面



設定画面内 [Add]、[Edit] ボタンをクリックし、[Group Configuration] ダイアログボックスを表示し、指定グループ名に対して共通設定内容よりも高優先の個別指定をします。
グループ名を指定後に、左欄より設定内容を選択し、専用画面を通じて入力編集します。
リストに表示のグループは上位行ほど優先されます。[Move up],[Move down]ボタンで操作します。

ユーザが複数グループに所属する場合の扱いについて：

a)設定項目："SFTP Directories", "Mapped Drivers"

・**"Use first applicable group"選択時：**

～リストの中で最上位の該当グループの内容が適用されます。

・**"Use all applicable groups"選択時：** *…〈7.2 SP1 から追加〉*

～リスト中 該当全グループの内容が適用されます。但し 下記詳細条件を配慮します。

①"User login directory"は、リスト中最上位グループの指定内容に従う。

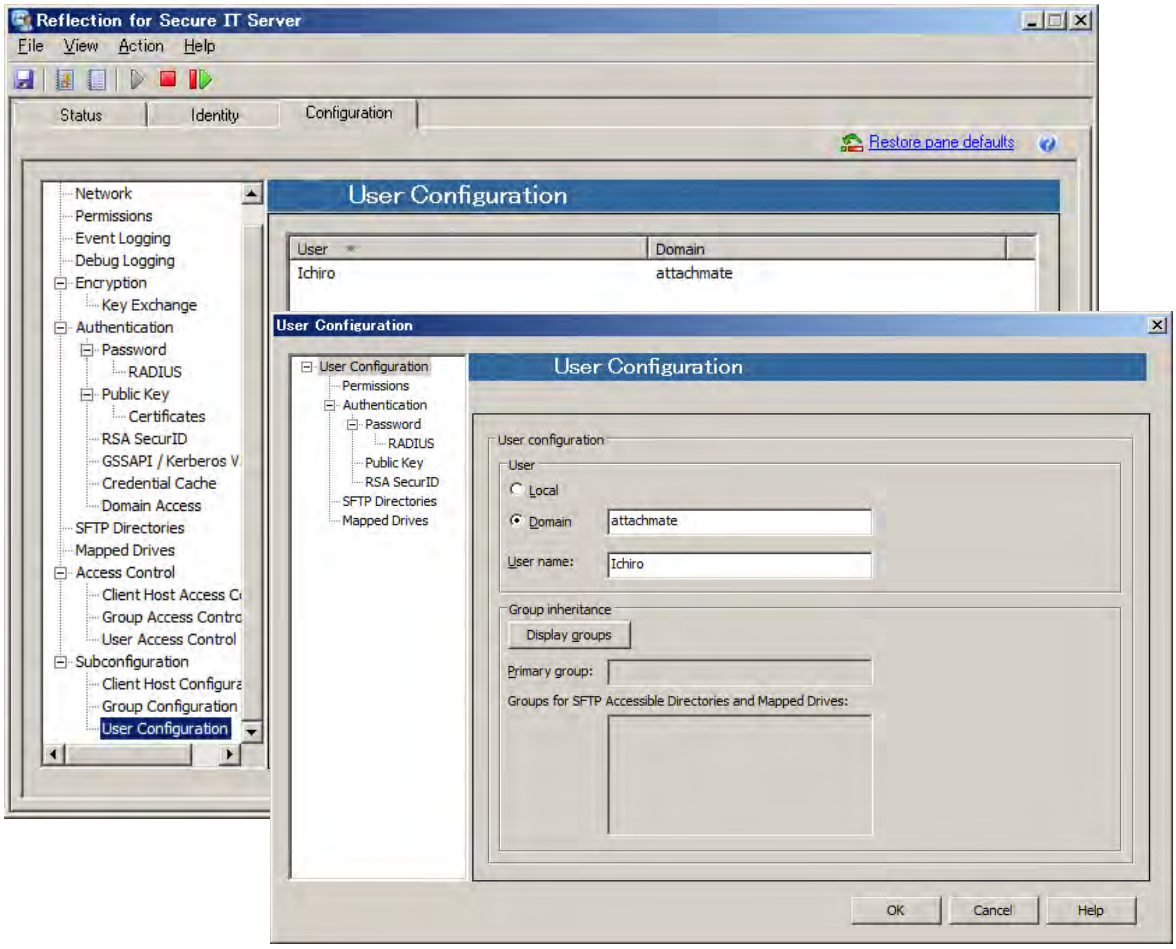
②"Inherit directories","Inherit drivers" を非選択時には、その内容は継承せず。

③同一"Virtual directory"名称が重なった場合、リスト中上位のグループ内容を適用。

b)設定項目："Permissions", "Authentication"

～常にリストの中で最上位の該当グループの内容が適用されます。

4.2.26 [User Configration] 設定画面



設定画面内［Add］、［Edit］ボタンをクリックし、［User Configuration］ダイアログボックスを表示し、指定ユーザ名に対して共通設定内容よりも高優先の個別指定をします。

ユーザ名を指定後に、左欄より該当設定画面を選択し、専用の設定画面を通じて入力編集します。