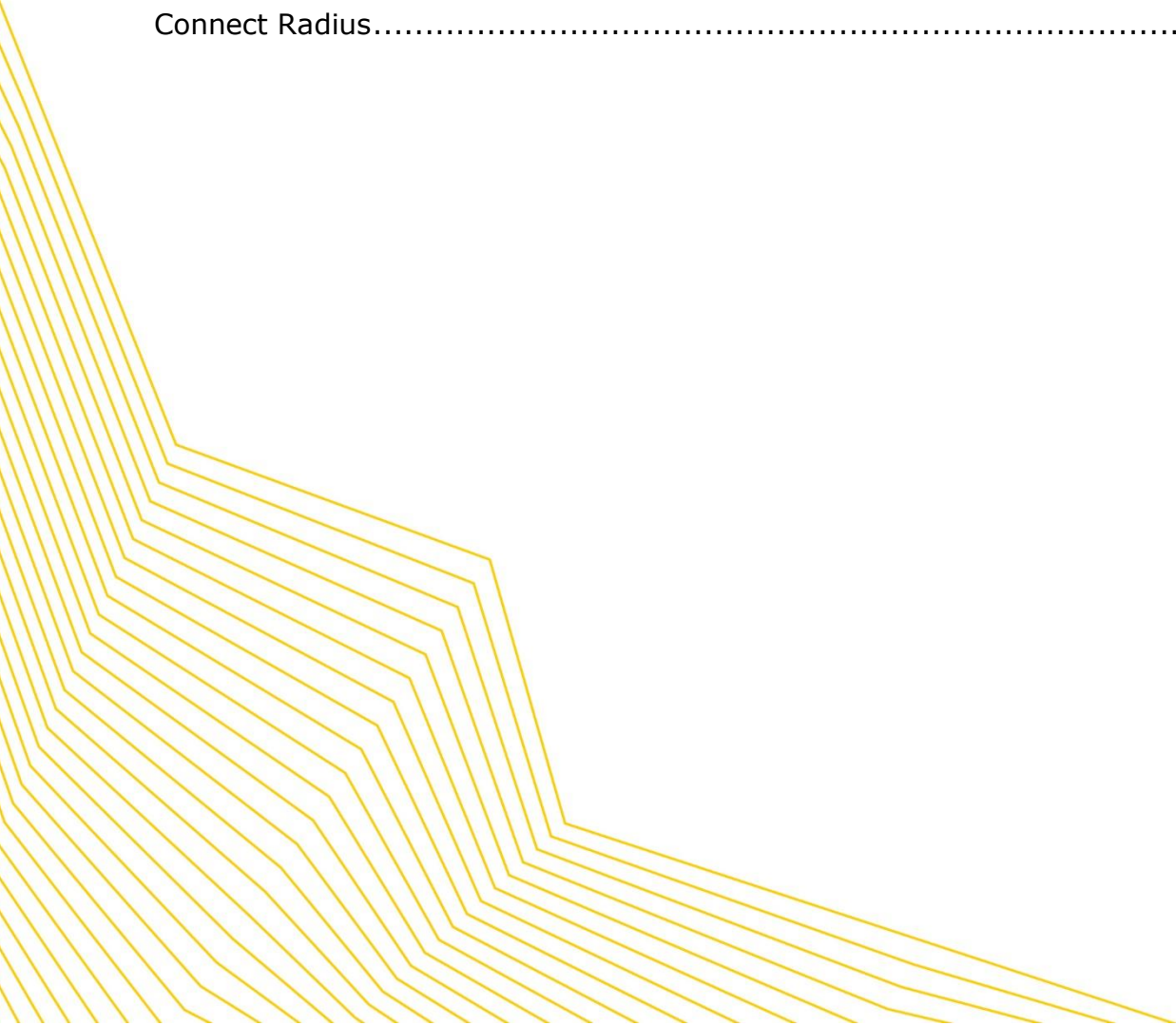




## Bintec/Teldat VPN gateway configuration

### Contents

Bintec/Teldat VPN gateway configuration for SMS PASSCODE .....	1
Connect Radius.....	1





## Bintec/Teldat VPN gateway configuration for SMS PASSCODE

In this scenario about the VPN configuration on the Bintec gateway, an IPsec peer configuration entry is created which allows the simultaneous connection of multiple clients (IPsec Multi-User). Following the IPsec pre-shared key authentication, the One-Time Passcode (OTP) authentication between the Bintec VPN client and the SMS PASSCODE™ server is completed via a RADIUS server, in this case a Microsoft Network Policy Server (NPS).

### Note

Instead of the **Multi-User IPsec configuration**, there is also the option to create a separate IPsec peer configuration entry for each VPN client. The priority of the Multi-User IPsec peer must always be lower than other IPsec peer configuration entries.

## Connect Radius

To connect the RADIUS server to the Bintec VPN gateway, go to the following menu:

1. Go to **System Management -> Remote Authentication -> RADIUS ->New.**

The screenshot shows the configuration window for a new RADIUS entry. The left sidebar contains a navigation menu with 'Remote Authentication' selected. The main window has tabs for 'RADIUS', 'TACACS+', and 'Options'. The 'Basic Parameters' section includes the following fields:

Authentication Type	XAUTH
Server IP Address	172.16.105.131
RADIUS Secret	••••••••
Default User Password	••••••••
Priority	0
Entry active	<input checked="" type="checkbox"/> Enabled
Group Description	Default Group 0

Below the 'Basic Parameters' section is an 'Advanced Settings' section, which is currently collapsed. At the bottom of the window are 'OK' and 'Cancel' buttons.

### System Management->Remote Authentication->RADIUS->New

Proceed as follows:

1. Select **Authentication Type XAUTH** in order to enable authentication via the Windows Server.
2. Enter the **Server IP Address**, e.g. *172.16.105.131* , to communicate with the Microsoft RADIUS server.
3. Enter the shared password used for communication between the RADIUS server and your device, e.g. *supersecret* .
4. Press **OK** to confirm your entries.



An address pool must be created to assign an IP pool to the VPN profile of the Multi-User IPSec peer.

## 1. Go to **VPN -> IPSec -> IP Pools -> Add**

The screenshot shows the 'IPSec Peers' configuration page with the 'IP Pools' tab selected. A dialog box for adding a new IP pool is displayed. The 'IP Pool Name' field contains 'IPSec-Pool' and the 'IP Pool Range' field contains '10.10.10.1 - 10.10.10.100'. The 'Add' button is highlighted.

## **VPN -> IPSec -> IP Pools -> Add**

Proceed as follows:

1. Enter the name of the IP pool for **IP Pool Name**, e.g. *IPSec-Pool*.
2. For **IP Pool Range**, enter the first IP address of the address pool in the first field, e.g. *10.10.10.1*.
3. Enter the last IP address of the address pool in the second field, e.g. *10.10.10.100*.
4. Click **Add**.

A profile must then be created in order to be able to refer to the RADIUS server.

Go to **VPN -> IPSec -> XAUTH Profiles -> New**.

The screenshot shows the 'XAUTH Profiles' configuration page with the 'New' dialog open. The 'Basic Parameters' section is visible with the following values: Description: 'SMS-Passcode', Role: 'Server', Mode: 'RADIUS', and RADIUS Server Group ID: 'STR\_defaultGroup0'. The 'OK' button is highlighted.

## **VPN -> IPSec -> XAUTH Profiles-> New**

Proceed as follows to set up a profile:

1. Enter a **Description** for this XAuth profile, e.g. *SMS Passcode*.



2. Select the **Role** of the gateway for the XAuth authentication; in this instance, *Server*.
3. Under **Mode** select *RADIUS*. Authentication is carried out via the RADIUS server.
4. Confirm with **OK**.

Now the actual **IPSec Peer** is created.

1. Go to **VPN -> IPSec -> IPSec Peers -> New**

The screenshot shows the configuration page for a new IPSec Peer. The left sidebar contains a navigation menu with categories like Assistants, System Management, Physical Interfaces, LAN, Wireless LAN Controller, Networking, Routing Protocols, Multicast, WAN, VPN, and Monitoring. The main content area is titled 'IPSec Peers' and has several tabs: Phase-1 Profiles, Phase-2 Profiles, XAUTH Profiles, IP Pools, and Options. The 'Peer Parameters' section is active, showing a form with the following fields:

- Administrative Status:  Up  Down
- Description: SMS-Passcode-Users
- Peer Address: (empty)
- Peer ID: Fully Qualified Domain Name (FQDN) (dropdown)
- Internet Key Exchange: IKEv1 (dropdown)
- Preshared Key: (masked with dots)
- Interface Routes: (empty)
- IP Address Assignment: IKE Config Mode Server (dropdown)
- Config Mode:  Pull  Push
- IP Assignment Pool: IPSec-Pool (dropdown)
- Local IP Address: 172.16.105.141
- Additional Traffic Filter: (table with columns: Description, Protocol, Src. IP/Mask/Port, Dest. IP/Mask/Port, and an Add button)

The 'Advanced Settings' section is also visible, containing:

- Advanced IPSec Options:
  - Phase-1 Profile: None (use default profile) (dropdown)
  - Phase-2 Profile: None (use default profile) (dropdown)
  - XAUTH Profile: SMS-Passcode (dropdown)
  - Number of Admitted Connections:  One User  Multiple Users
  - Start Mode:  On Demand  Always up
- Advanced IP Options:
  - Back Route Verify:  Enabled
  - Proxy ARP:  Inactive  Up or Dormant  Up only
- IPSec Callback:
  - Mode: Inactive (dropdown)

At the bottom of the form are 'OK' and 'Cancel' buttons.

## VPN -> IPSec -> IPSec Peers -> New

Proceed as follows:

1. Enter a **Description** of the peer which identifies it, e.g. *SMS Passcode User*.
2. In this scenario, no IPSec peer ID is saved to enable the Multi-User IPSec connections.
3. Under **Preshared Key** enter the password agreed with the peer, e.g. *supersecret*.
4. For **IP Address Assignment**, select the configuration mode of the interface; in this instance, *Server In IKE Configuration Mode*.
5. Select a configured **IP Assignment Pool**, e.g. *IPSec Pool*.
6. Enter the LAN IP address of the VPN gateway under **Local IP Address**, e.g. *172.16.105.141*.
7. Click **Advanced Settings**.



8. If selecting *None (Use Standard Profile)*, the profile indicated as standard in **Phase 1 Profile/Phase 2 Profile** is used.
9. Select the **XAUTH Profile** that has already been configured, e.g. *SMS Passcode*.
10. For **Number of Admitted Connections**, set it to *Multiple Users* to enable IPSec Multi-User mode.
11. Leave the remaining settings unchanged and confirm them with **OK**.