

Remote Access Documentation

Problem Description

- End user needs a new HRA account and/or is not able to connect receiving the next error message: "".

Procedure

- Go to <https://ipcreg.honeywell.com/IPCREG/hgr/jsp/main.jsp> and enter EU's EID in the Request Account /Check Status section and click on "Check Status" button

Honeywell Information Technology Services (HITS)

Welcome to the NEW IPC Registration site

Request Account/Check Status

EID

(for account being requested)

Click here to view the Data Privacy Notice.

To request an IPC account, the following information is required:

- EID of the user for the account being requested. "Need to look up an EID?"
- The Work Region of the user.
- The IPC Access Group Type and Group Name if the access group type is restricted/special.

Administration Services

EID

LDAP Password ?

- Need to approve an account?
- Need to approve a group request?
- Need to revoke an account?
- Need reporting?
- Need to create/edit a special or restricted access group?

Account Status

Requestor EID	: E320130	Requestor Company	: Honeywell
Request for	: Special	Group Name	: HGR ADMIN
Final Approver EID	: E605042	Manager EID	: E061087
Initially Requested on	: 09/15/2005	Approver Comments	: -
Request Status	: Account Active	Status Changed on	: 09/15/2005

Note: The EID requested already has an active IPC account. If the IPC password has been forgotten or lost, please contact the helpdesk so that it can be reset

- If you can see the "Account Status" information validate that request status is "account active", if so send the ticket to US-GBL-HGRA queue

DRAFT

Honeywell Confidential

- If you can see the legend "There are no pending requests for EID provided" Then request a new account clicking on place request.

Honeywell Information Technology Services (HITS)

Welcome to the NEW IPC Registration site

Request Account/Check Status

EID
(for account being requested)

Click here to view the Data Privacy Notice.

To request an IPC account, the following information is required:

- EID of the user for the account being requested."Need to look up an EID?"
- The Work Region of the user.
- The IPC Access Group Type and Group Name if the access group type is restricted/special.

Administration Services

EID

LDAP Password ?

- Need to approve an account?
- Need to approve a group request?
- Need to revoke an account?
- Need reporting?
- Need to create/edit a special or restricted access group?

There are no pending requests for the EID provided.

- Fill out the form; select standard access type unless the end user states that he needs access to a special group. Select continue

Honeywell Information Technology Services (HITS)

Place Request

EID for account

Manager EID *

Work Region *

Access Type *

Business Justification *

Note :

- * indicates mandatory

Manager EID
Manager of the EID for whom the account is being requested.

Work Region
Please note that your Work Region will be pulled from current Honeywell records unless it is not present. Please select your Work Region if it does not automatically populate.

Access Type
Choose either "Standard" or "Restricted/Special". Generally Honeywell employees should choose "Standard". Requester's who require special or restricted network access such as DSES employees, must select "Restricted/Special". If you have any questions please consult your Manager. All non-Honeywell users should consult with their Honeywell Manager/Approver on the access type to select.

Access Group Name
Requesters who require "Restricted/Special" access, must choose one of the existing Access Group Names. If you have any questions please consult your Honeywell Manager/Approver.
For new DSES requests please fill out the ITAR form which can be found at:
<http://web.das.honeywell.com/security/dsesinstructions.htm>
Please forward that to group owner for quicker turnaround.

Company Name
For non-Honeywell employees, this is the company for who the account is being requested.

Business Justification
Enter a business justification as to why you need this remote access solution. Note: This information will be submitted as part of the email to the Approver you selected.

You will see the terms and conditions page, click on accept.

Terms & Conditions

Honeywell Remote Access user Agreement

All users of Honeywell Information Systems and computing assets are to follow the Honeywell Information Systems Security Policy and abide by the Appropriate Use policy for their use. Remote access and wireless services users are required to follow the usage standard for remote access and wirelessly connecting to the Honeywell network.

In order to connect with and use Honeywell systems and services, you first must have Honeywell VPN access rights.

For All users of Honeywell VPN technology:

All connectivity shall be within the established Honeywell VPN connection while attached to the Honeywell network. Split tunneling, and multiple simultaneous VPN sessions with connections outside of the Honeywell network are prohibited.

For iPC client users:

- No installation of any non-Honeywell approved VPN technology is to be performed due to identified risk from non-trusted and uncertified VPN client software.
- The iPC solution uses PKI certificates for authentication. The use and protection of these certificates is the sole responsibility of the end user. Users are not to share their certificate, associated files, or information protecting it, with anyone.
- All security settings configured in the Honeywell VPN client software at installation time are not to be changed.
- iPC users must have personal firewall software and updated anti-virus software installed and running. The iPC client installation package meets the policy requirements by including a personal firewall application with each installed instance. Users of Honeywell corporate issued units with a standard machine image will have the McAfee Anti-Virus software included. The iPC client interrogates installed systems for any of the following AV products; McAfee, TrendMicro or Norton AV applications. If any of these are found to be installed and functioning, the iPC client will successfully load and communicate. Users are required to have an operational and up-to-date anti-virus application on the computing appliance in accordance with Honeywell security policy.
- As required by Honeywell Information Systems Policy & Standards, all connecting computing appliances must have up-to-date anti-virus software programs installed and operational.
- iPC users must receive approval from a Honeywell employee who is your immediate supervisor/Manager.
- An identified conflict exists between the authorized iPC VPN client and the installation of any other VPN clients. This creates a limitation on the installed computing appliance that only one operating VPN client can be resident on each machine. This client software conflict may force a problem resolution to utilize multiple computing platforms, or unique operating system configurations to address this issue.

Accessing Honeywell Networks and Systems

You are accessing Honeywell International Inc. information resources. This system is restricted solely to Honeywell authorized users for business related purposes in accordance with Honeywell policies. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Violators may be subject to disciplinary and/or legal action. The use of this system may be monitored and recorded for security, administrative or other purposes. By proceeding to log on, you expressly consent to such monitoring and/or recording.

5. Automatic email will be sent to end user's manager and after approval new account will be ready to use it.